Dominion KX

User Manual

DKX116
DKX216
DKX232

CE c UL us LISTED 1F61 I.T.E.

Copyright ©2004 Raritan Computer, Inc.

KX-0A-E
August 2003
255-80-6040

Raritan Computer Inc.
400 Cottontail Lane
Somerset, NJ 08873
USA
Tel. 1-732-764-8886
Fax. 1-732-764-8887
E-mail: sales@raritan.com
http://www.raritan.com/

Raritan Computer Europe, B.V.
Eglantierbaan 16
2908 LV Capelle aan den IJssel
The Netherlands
Tel. 31-10-284-4040
Fax. 31-10-284-4049
E-mail: sales.europe@raritan.com
http://www.raritan.com/

Raritan Computer Japan, Inc.
Kuga Building 7F
11-6, Kuramae 4-chome
Taitoo-ku, Tokyo 111-0051
Japan
Tel. 81-3-5833-6360
Fax. 81-3-5833-6336
E-mail: sales.japan@raritan.com
http://www.raritan.co.jp

Raritan Computer Taiwan, Inc.
5F, 121, Lane 235,
Pao-Chiao Rd., Hsin Tien
Taipei Hsien
Taiwan, ROC
Tel. 886-2-8919-1333
Fax. 886-2-8919-1338
E-mail: sales.asia@raritan.com
http://www.raritan.com.tw

Raritan Computer France
120 Rue Jean Jaures
93200 Levallois-Perret
France
Tel. 33-14-756-2039
Fax. 33-14-756-2061
E-mail: sales.france@raritan.com
http://www.raritan.fr

Raritan Computer Deutschland GmbH
Lichstraße 2
D-45127 Essen
Germany
Tel. 49-201-747-9820
Fax. 49-201-747-9850
E-mail: sales.germany@raritan.com
http://www.raritan.de

Raritan Computer U.K. Ltd.
Unit 1 Cobbett Park, Moorfield Road
Guilford, Surrey, GU1 RU
United Kingdom
Tel. 44-1483-457788
Fax. 44-1483-46987
E-mail: sales.uk@raritan.com
http://www.raritan.com

Shanghai Representative Office of Raritan Computer, Inc.
RM 19C-1 Shanghai Shiye Building
18 Caoxi North Road
Shanghai China 2000030
Tel. 86-21-64680475
Fax. 86-21-64627964
E-mail: mailto:sales.asia@raritan.com
http://www.raritan.com.tw/

Raritan®

This page intentionally left blank.

FCC Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential environment may cause harmful interference.

Trademark Information

Product names mentioned in this document are trademarks or registered trademarks of their respective companies. Dominion, IP-Reach, Paragon, MasterConsole, and their respective logos are trademarks or registered trademarks of Raritan Computer, Inc. PS/2, RS/6000, and PC/AT are registered trademarks of International Business Machines Corporation. Sun is a registered trademark of Sun Microsystems. Microsoft and Windows are registered trademarks of Microsoft Corporation. All other marks are the property of their respective owners.

Japanese Approvals

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

For assistance in the U.S., please contact the Raritan Technical Support Team at (732) 764-8886 or e-mail us at support@raritan.com

Ask for Technical Support – Monday through Friday, 8:00am to 8:00pm, EST.

For assistance internationally, please contact your regional Raritan office.

Important Information

Login

- The default Dominion KX login user name is **admin** and the password is **raritan**. This user has administrative privileges.
- Passwords are case sensitive and must be entered in the exact case combination in which they were created.
- The default password **raritan** must be entered entirely in lowercase letters.
- To ensure security, change the default password as soon as possible.

Default IP Address

- Dominion KX ships with the default IP address of 192.168.0.192.

Table of Contents

Chapter 1: Introduction 1

Dominion KX Overview 1
Product Photos 2
Product Features 3
Terminology 4
Package Contents 4

Chapter 2: Installation 5

Configuring Target Servers 5
- Server Video Resolution 5
- Desktop Background 5
- Windows XP / Windows 2003 Settings 5
- Windows 2000 / ME Settings 6
- Windows 95 / 98 / NT Settings 6
- Linux Settings 6
- Sun Solaris Settings 6
- Apple Macintosh Settings 7

Configuring Network Firewall Settings 7
Physical Connections 8
Initial Configuration 9
Note to CommandCenter Users 10
Connect to Dominion KX Remotely 10
- Launch Raritan Remote Client (RRC) 10
- Establish a Connection 11

Chapter 3: Raritan Remote Client (RRC) 13

Invoking RRC via Web Browser 13
- Security Settings 13
- Launching RRC 13
- Removing RRC From the Browser Cache 14

Optional: Installing RRC Software 15
RRC Window Layout 15
RRC Navigator 16
- Navigator Options 17
- Creating New Profiles 17
- Establishing a New Connection 19
- Closing a Remote Connection 19

RRC Toolbar and Shortcuts 20
RRC Status Bar 21
Remote KVM Console Control 22
Single Mouse Mode / Dual Mouse Mode 22
- Full Screen Mode 23
- Keyboard Macros 24
- Connection and Video Properties 27
- Connection and Video Properties 27
- Color Calibration 29

Select Administrative Functions via RRC 30
- Firmware Upgrade 30
- Device Restart 30
- Device Configuration Backup and Restore 30
- Log Files 30

Chapter 4: Administrative Functions 31

Launching Dominion KX Manager 31
Dominion KX Manager Interface 32
Network Configuration 32
System-Level Security Parameters 34
Users, Groups, and Access Permissions 36
- Overview 36
- Relationship Between Users and Group Entries 36
- Create or Edit User Groups and Access Permissions 37
- Delete User Groups 38
- Create or Edit Users 38
- Delete Users 39

Remote Authentication....39
Introduction....39
Remote Authentication Implementation....39
General Settings for Remote Authentication....41
View Dominion KX Event Log (Status)....43
Forced User Logoff....44
Reboot Dominion KX....44
Performance Settings....44
Time and Date....45
Chapter 5: Local Console Port Access....47
Local Port Functionality....47
Selecting Servers....48
Local Port Administration....49
Appendix A: Specifications....51
Remote Connection....51
Raritan Remote Client (RRC) Applet....51
Dominion KX Manager (Remote Administration Applet)....51
TCP Ports Used....52
KVM Input....52
Appendix B: Frequently Asked Questions....53
General Questions....53
Remote Access....53
Ethernet Networking....55
Servers....57
Installation....58
Local Port....59
Power Control....60
Scalability....61
Computer Interface Modules (CIMs)....61
Security....62
Manageability....62
Miscellaneous....63

Table of Figures

Figure 1 Dominion KX Configuration 1
Figure 2 Dominion KX Front and Rear Panels 2
Figure 3 Dominion KX Computer Interface Module (CIM) 2
Figure 4 Terminology and Topology 4
Figure 5 Solaris Mouse Configuration Window 6
Figure 6 Back Panel of Dominion KX 8
Figure 7 RRC Connection Window 10
Figure 8 RRC Screen 11
Figure 9 Type the IP Address of your Dominion KX unit 13
Figure 10 RRC Loading Screen 13
Figure 11 Possible Security Alert Screens 14
Figure 12 RRC Screen Components 15
Figure 13 Expanded RRC Navigation Tree 16
Figure 14 Connection Profile Window 17
Figure 15 Connect tab 18
Figure 16 Security tab 19
Figure 17 RRC Toolbar 20
Figure 18 RRC Status Bar Components 21
Figure 19 Navigation Tree 22
Figure 20 Remote Desktop, where dual mouse cursors will appear 22
Figure 21 Standard View 23
Figure 22 Full Screen Mode 23
Figure 23 Add Keyboard Macro Window 24
Figure 24 Add Keyboard Macro Window 25
Figure 25 Keyboard Macros Window 25
Figure 26 Minimize All Window Menu Option 26
Figure 27 Modify Connection Window 27
Figure 28 Settings Window 28
Figure 29 Example of Sizing the Notepad Window 29
Figure 30 Dominion KX Manager Login Screen 31
Figure 31 Network Configuration Window 32
Figure 32 Access Control List Window 33
Figure 33 Security Configuration Window 34
Figure 34 Groups Window 37
Figure 35 Select Ports Window 37
Figure 36 Access Control List Window 38
Figure 37 Create/Edit User Window 38
Figure 38 Authorization Flow Diagram 40
Figure 39 Remote Authentication Window 41
Figure 40 Dominion KX Status Window 43
Figure 41 Logoff User Menu, accessed by Right-clicking on User icon 44
Figure 42 Performance Settings Window 44
Figure 43 Time and Date Window 45
Figure 44 Local User Panel on Dominion KX 47
Figure 45 Local Server Display 48
Figure 47 Administrative Menu 49
Figure 48 Channel Configuration Menu 49
Figure 49 Network Settings Menu 50
Figure 50 Help Menu 50
Figure 51 System Information Window 50

This page intentionally left blank.

Chapter 1: Introduction

Dominion KX Overview

Dominion KX is an enterprise-class, secure, digital KVM switch that provides BIOS-level access and control of 32 servers from anywhere in the world via Web browser. At the rack, Dominion KX provides BIOS-level control of up to 32 servers and other IT devices from a single keyboard, monitor, and mouse. Dominion KX's integrated remote access capabilities provide the same BIOS-level control of your servers, from anywhere in the world, via Web browser.

Dominion KX is easily installed using standard UTP (Cat 5/5e/6) cabling. Its advanced features include 128-bit encryption, remote power control, dual Ethernet, LDAP, RADIUS, Active Directory, SNMP, and syslog integration, and Web management. These features enable you to deliver higher uptime, better productivity, and bulletproof security – at any time from anywhere.

For larger data centers and enterprises, multiple Dominion KX units (along with Dominion SX units for remote serial console access and Dominion KSX for remote/branch office management) can be integrated into a single logical solution via Raritan's CommandCenter management appliance.

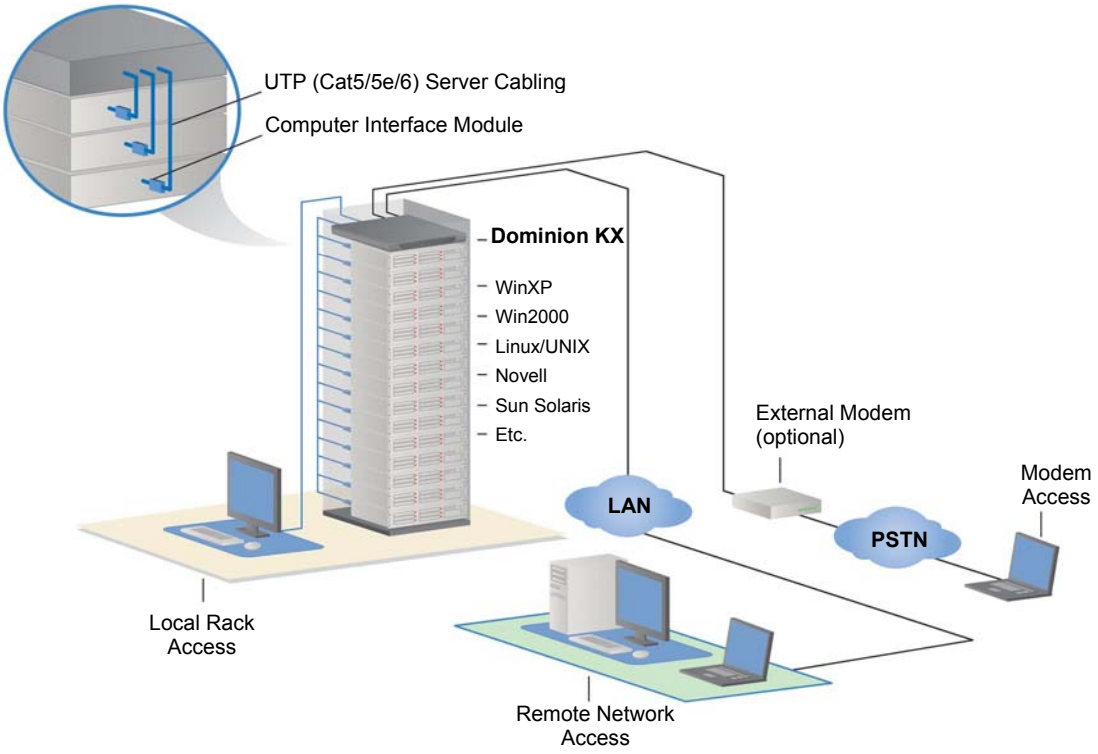

Figure 1 Dominion KX Configuration

Product Photos

Figure 2 Dominion KX Front and Rear Panels

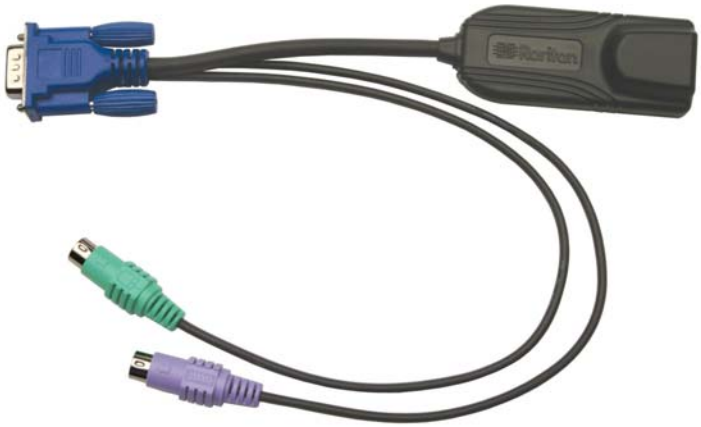

Figure 3 Dominion KX Computer Interface Module (CIM)

Product Features

Hardware

- 1U rack-mountable (brackets included)
- 16 or 32 server ports
- Multiple User Capacity
- UTP (Cat5/5e/6) Server Cabling
- Dual failover 10/100 LAN
- Modem-ready via external Modem Port
- FLASH upgradeable
- Auto-switching power supply
- Local User Port for Rack Access
  - PS/2 and USB keyboard/mouse ports
  - Fully concurrent with remote users
  - On-Screen display
- Centralized access security
- Integrated Power Control
- LED indicators for power, network activity, and remote user status
- Integrated KVM Over IP Remote Access
- Cross-platform server support

Software

- Plug and Play Appliance
- Web based access and management
- Intuitive Graphical User Interface
- Integration with Raritan's CommandCenter management appliance
- High-color (15-bit+) palette support
- 128-bit encryption of complete KVM signal, including video
- LDAP, RADIUS, or Active Directory – or Internal Authentication
- DHCP or fixed IP addressing

Terminology

This manual uses of the following terms for components of a typical Dominion KX configuration. Please refer to the diagram below for clarification, if needed.

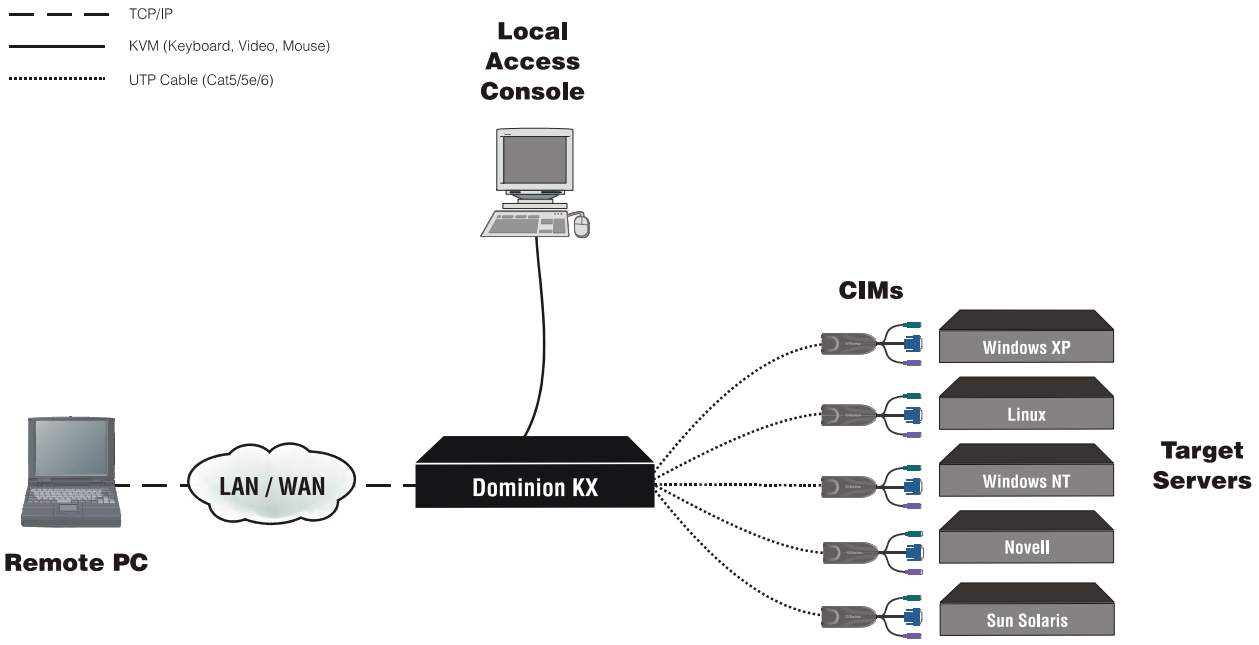

Figure 4 Terminology and Topology

Target Servers	Servers with graphical video cards and user interfaces (e.g., Windows, Linux, Solaris, etc.) to be accessed remotely via Dominion KX.
Remote PC	A networked Windows-based computer used to access and control target devices connected to Dominion KX.
Local Access Console	An optional user console, consisting of a keyboard, mouse, and multi-sync VGA monitor, directly attached to Dominion KX to control target servers locally (directly at the rack, not through the network).
CIM (Computer Interface Modules)	Server dongles (Raritan P/N DCIM-xxxx) that connect to each target server. Available for PS/2, Sun, USB, and Sun USB keyboard and mouse ports.

Package Contents

Dominion KX ships as a fully configured stand-alone product in a standard 1U 19" rackmount chassis. Each Dominion KX unit ships with the following contents:

(1) Dominion KX unit
(1) Dominion KX printed Quick Setup Guide
(1) Raritan User Manual CD-ROM
(1) Raritan Remote Client software CD-ROM
(1) Rackmount Kit
(1) AC Power Cord
(1) Cat5 Network cable
(1) Cat5 Network crossover cable
(1) Set of 4 rubber feet (for desktop use)

Chapter 2: Installation

Configuring Target Servers

Before installing Dominion KX, you must configure any target servers to be accessed via Dominion KX, to ensure optimum performance. Note that the following configuration requirements apply only to *target servers*, not to the client workstations (Remote PCs) that you use to access Dominion KX remotely (see **Chapter 1: Introduction**, ***Terminology*** for more information).

Server Video Resolution

Ensure that each target server's video resolution and refresh rate is supported by Dominion KX and that the signal is non-interlaced. Dominion KX supports the following video resolutions:

640 x 480 @ 60Hz	1024 x 768 @ 60Hz
640 x 480 @ 72Hz	1024 x 768 @ 70Hz
640 x 480 @ 75Hz	1024 x 768 @ 75Hz
640 x 480 @ 85Hz	1024 x 768 @ 77Hz
	1024 x 768 @ 85Hz
720 x 400 @ 70Hz	
720 x 400 @ 85Hz	1152 x 864 @ 60Hz
	1152 x 864 @ 70Hz
800 x 600 @ 56Hz	1152 x 864 @ 75Hz
800 x 600 @ 60Hz	
800 x 600 @ 72Hz	1152 x 900 @ 66Hz
800 x 600 @ 75Hz	
800 x 600 @ 85Hz	1280 x 960 @ 60Hz
	1280 x 1024 @ 60Hz

Desktop Background

For optimal bandwidth efficiency and video performance, target servers running graphical user interfaces such as Windows, Linux, X-Windows, Solaris, and KDE should be configured with desktop backgrounds set to a predominantly solid, plain, light-colored graphic. The desktop background need not be *completely* solid; but desktop backgrounds featuring photos or complex gradients should be avoided.

Windows XP / Windows 2003 Settings

On target servers running Microsoft Windows XP, disable the **Enhanced Pointer Precision** option, and set the mouse motion speed exactly to the middle speed setting. These parameters are found in **Control Panel → Mouse → Mouse Pointers**.

Disable transition effects in **Control Panel → Display → Appearance → Settings**.

Note: *For target servers running Windows NT, 2000, or XP, you may wish to create a user name that will be used only for remote connections through Dominion KX. This will enable you to keep the target server's slow mouse pointer motion/acceleration settings exclusive to the Dominion KX connection only.*

Note: *Windows XP and 2000 login screens revert to pre-set mouse parameters that differ from those suggested for optimal Dominion KX performance. As a result, mouse sync will not be optimal at these screens. If you are comfortable adjusting the registry on Windows target servers, you can obtain better Dominion KX mouse synchronization at login screens by using the Windows registry editor to change the following settings: Default user mouse motion speed = 0; mouse threshold 1= 0; mouse threshold 2 = 0.*

Windows 2000 / ME Settings

On target servers running Microsoft Windows 2000/ME, set the mouse pointer acceleration to **None** and the mouse motion speed exactly to the middle speed setting. These parameters are found in **Control Panel → Mouse**.

Disable transition effects in **Control Panel → Display → Effects**.

Windows 95 / 98 / NT Settings

On target servers running Microsoft Windows 95/98/NT, set the mouse motion speed to the slowest setting in **Control Panel → Mouse → Motion**.

Disable window, menu, and list animation in **Control Panel → Display → Effects.**

Linux Settings

On target servers running Linux graphical interfaces, set the mouse acceleration to exactly 1 and set threshold to exactly 1.

Ensure that each target server running Linux is using a resolution supported by Dominion KX at a standard VESA resolution and refresh rate. Each Linux target server should also be set so the blanking times are within +/- 40% of VESA standard values.

To check for these parameters:

1. Go to the Xfree86 Configuration file XF86Config
2. Using a text editor, disable all non-Dominion KX supported resolutions
3. Disable the virtual desktop feature, which is not supported by Dominion KX
4. Check blanking times (+/- 40% of VESA standard).
5. Restart computer

Note: *In many Linux graphical environments, the command <**Ctrl+Alt+Plus**> will change the video resolution, scrolling through all available resolutions that remain enabled in the XF86Config file.*

Sun Solaris Settings

On target servers running the Solaris operating system, set the mouse acceleration value to exactly 1 and threshold to exactly 1.

This can be performed from the graphical user interface, or with the command line:

```
xset mouse a t
```

where "`a`" is the acceleration and "`t`" is the threshold.

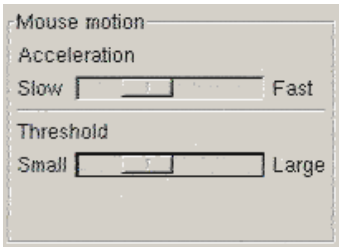

Figure 5 Solaris Mouse Configuration Window

All target servers must be configured to one of the display resolutions supported by Dominion KX, as listed in the beginning of this chapter. The most popular supported resolutions for Sun machines are:

1024x768@60Hz
1024x768@70Hz
1024x768@75Hz
1024x768@85Hz
1152x900@66Hz
1152x900@76Hz
1280x1024@60Hz

Target servers running the Solaris operating system must output VGA video (H-and-V sync, not composite sync). To change your Sun video card output from composite sync to the non-default VGA output, first issue the **Stop+A** command to drop to bootprom mode. Then, issue the command:

```
setenv output-device screen:r1024x768x70
```

to change the output resolution. Issue the "**boot**" command to reboot the server.

Alternatively, you may contact your Raritan representative to purchase a video output adapter. 13W3 Suns with composite sync output require APSSUN II Guardian converter for use with Dominion KX. HD15 Suns with composite sync output require the 1396C converter to convert from HD15 to 13W3 and an APSSUN II Guardian converter to support composite sync. HD15 Suns with separate sync output require an APKMSUN Guardian converter for use with Dominion KX.

Apple Macintosh Settings

For target servers running an Apple Macintosh operating system, no specific mouse setting is required. However, when using Dominion KX to access and control your target server, you must set the Dominion KX client (Raritan Remote Client) to "single cursor" mode (see **Chapter 3: Raritan Remote Client, *Remote KVM Console Control, Single Mouse Mode***).

Dual cursor mode is not supported for Macintosh target servers; the two mouse pointers will not appear in sync if you attempt to control a Macintosh server via Dominion KX in dual cursor mode.

Configuring Network Firewall Settings

If you wish to access Dominion KX through a network firewall, your firewall must allow communication on TCP Port 5000. Dominion KX can also be configured to use a different TCP port of your designation (see **Chapter 4: Administrative Functions, *Network Configuration***).

Optional: To take advantage of Dominion KX's web-access capabilities, the firewall must also allow inbound communication on TCP Port 443 – the standard TCP port for HTTPS communication. To take advantage of Dominion KX's automatic redirection of HTTP requests to HTTPS (i.e., so users may type the more common, "http://xxx.xxx.xxxx", instead of "https://xxx.xxx.xxxx"), then the firewall must also allow inbound communication on TCP Port 80 – the standard TCP port for HTTP communication.

Physical Connections

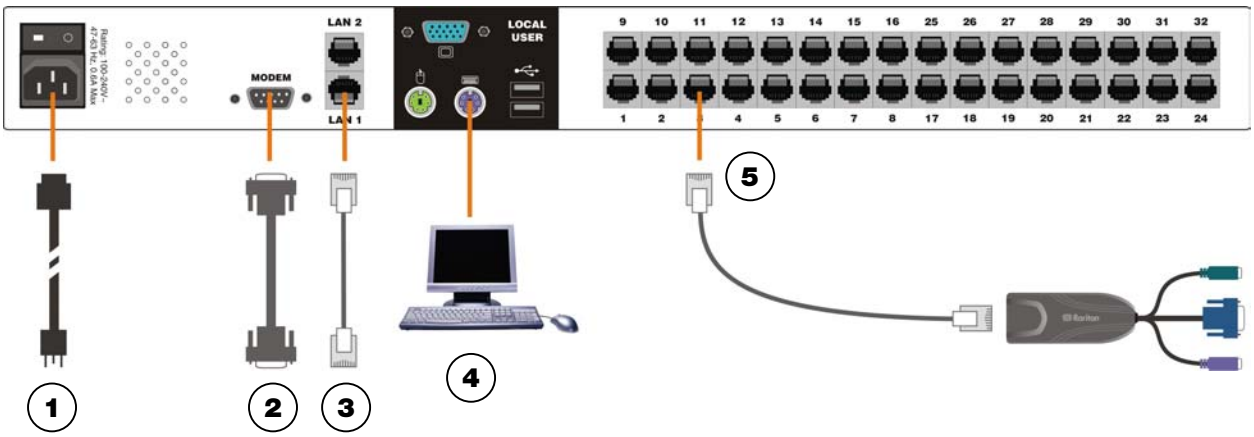

Figure 6 Back Panel of Dominion KX

1. AC Power Line

Attach the included AC power cord to Dominion KX and plug into an AC Power Outlet.

2. Modem Port (optional)

Dominion KX features a dedicated modem port for remote access even when the LAN/WAN is unavailable. Using a straight-through serial (RS-232) cable, connect an external serial modem to the port labeled MODEM on the back of Dominion KX (please see **Appendix A: Specifications** for a list of certified modems).

3. Network Ports

Dominion KX provides two Ethernet ports for failover purposes (not for load-balancing). By default, the LAN1 is active. In the case that the Dominion KX internal network interface or the network switch to which it is connected becomes unavailable, the port labeled LAN2 will become enabled, using the same IP address.

Connect a standard Ethernet cable (included) from the network port labeled LAN1 to an Ethernet switch, hub, or router. To make use of Dominion KX's Ethernet failover capabilities, you should also connect a standard Ethernet cable from the network port labeled LAN2 to an Ethernet switch, hub, or router.

4. Local Access Console Ports (optional)

For convenient access to target servers while at the rack, use Dominion KX's Local Access Console ports. Attach a multisync VGA monitor, mouse, and keyboard to the ports labeled Local User using either a PS/2 keyboard and mouse or a USB keyboard and mouse.

The USB keyboard and mouse ports are to be used only for keyboard and mouse access – other USB devices such as external drives, scanners, etc. should not be connected to these ports.

5. Server Ports

Dominion KX uses standard UTP cabling (Cat5/5e/6) to connect to each target server. The maximum cabling distance should not exceed 50ft (15m). To connect a target server to Dominion KX, use the appropriate Computer Interface Module (CIM:

DCIM-PS2	PS/2 keyboard/mouse
DCIM-SUN	Sun keyboard/mouse
DCIM-USB	USB keyboard/mouse
DCIM-SUSB	USB keyboard/mouse for Sun Microsystems servers

Attach the HD15 video connector of your CIM to the video card of your target server. Ensure that your target server's video has already been configured to a supported resolution and refresh rate. For Sun servers, also ensure that your target server's video card has been set to output standard VGA (H-and-V sync) and not composite sync.

Attach the keyboard/mouse connector of your CIM to the corresponding ports of your target server. Then, using a standard straight-through UTP (Cat5/5e/6) cable, connect the CIM to an empty server port on the back of your Dominion KX unit.

Initial Configuration

Assign an IP Address

1. Power ON Dominion KX via the power switch on the back of the unit.
2. Wait approximately 30 seconds as Dominion KX boots.
3. After it boots, a login prompt will appear on the monitor attached to Dominion KX's Local Access Console. Log on with the default username/password of **admin/raritan**.
4. Press the <**F5**> key to activate the Administrative Menu.
5. Select Option 3, **Network Settings**, and press the <**ENTER**> key.
6. Specify TCP/IP parameters for your Dominion KX unit: IP address, subnet mask, and default gateway. When finished, press the <**S**> key to save the settings, and then press <**ESC**> to exit the menu.
7. Press <**ESC**> again to log out. Power cycle your Dominion KX unit to enable the new network settings.
8. Connect one end of a straight-through Ethernet cable (included) to the port labeled **LAN1** on the rear panel of Dominion KX, and the other end to a network switch or router.
9. Reboot Dominion KX by switching the power OFF, then ON, in order to apply the new network settings.

Your Dominion KX unit is now network accessible.

Connect and Name Target Servers

1. Connect one end of a standard, straight-through UTP cable (Cat5/5e/6) to an unoccupied server port; connect the other end to the RJ45 port on a Dominion KX Computer Interface Module (CIM): DCIM-PS2 (PS/2 ports); DCIM-USB (USB ports); DCIM-SUSB (USB ports for Sun servers); or DCIM-SUN (Sun ports with HD15 video).
2. Connect the remaining ports on the CIM to the corresponding KVM ports of the server that you wish to manage using Dominion KX.
3. Repeat steps 1 and 2 to connect all servers that you wish to manage using Dominion KX.
4. On the Local Access Console, log on with the default username/password of **admin/raritan**.
5. Press the <**F5**> key to activate the Administrative Menu, and select Option 5, **Channel Configuration**.
6. Select a server port to rename, and press the <**ENTER**> key. When the cursor changes to a green color, assign a name (up to 20 characters) to identify the server connected to that port. Press <**ENTER**> to complete the change.
7. Press the <**S**> key to save your changes and then press <**ESC**> to exit the menu.

Change Default Password

1. Find and log on to any workstation with (a) network connectivity to your Dominion KX unit, and (b) Java Runtime Environment v1.4.x installed (Java Runtime Environment is available at http://java.sun.com/).
2. Launch a web browser such as Internet Explorer or Mozilla.
3. Enter the following URL: **http://IP-ADDRESS/admin**, where **IP-ADDRESS** is the IP address that you assigned to your Dominion KX unit.
4. The Dominion KX remote management tool, Dominion KX Manager, will launch. Log on with the standard username and password (**admin/raritan**). Immediately change the default password to one known only to you.

Note to CommandCenter Users

If you are using Dominion KX in a CommandCenter configuration, perform the installation steps as outlined above. After completing these steps, consult the CommandCenter user guide to proceed with your installation. The rest of this user guide applies primarily to users deploying their Dominion KX unit(s) without the integration functionality of CommandCenter.

Connect to Dominion KX Remotely

When you complete the physical installation of Dominion KX, establish an initial network connection, following the steps below.

*Note: Please see **Chapter 3: Raritan Remote Client, KVM Console Control** and **Color Calibration** for more information on optimizing Dominion KX performance for target servers.*

Launch Raritan Remote Client (RRC)

1. Log on to any Windows-based computer with network access to Dominion KX.
2. If you are using Windows NT, 2000, XP, or 2003, ensure that you are not a "restricted" user.
3. Launch Microsoft Internet Explorer (ensure that your Internet Explorer security settings allow the download and execution of ActiveX controls).

***Note:** A Windows default security setting of **Medium** is sufficient.*

4. In the Internet Explorer Address bar, type the IP address you assigned to Dominion KX in Step 6 of the previous section, **Initial Configuration.** Press the <**Enter**> key to load and launch the web access client, **Raritan Remote Client (RRC)**.

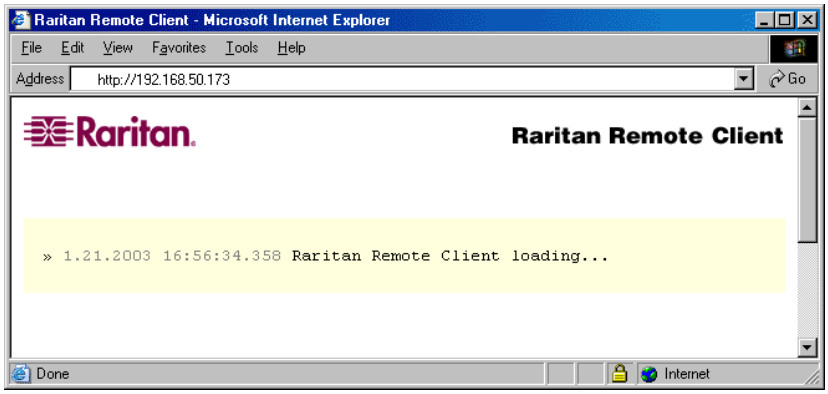

Figure 7 RRC Connection Window

5. After RRC launches, a device tree of all automatically detected Raritan devices found on your subnet is displayed on the left side of the screen. If you do not find your Dominion KX unit listed by name, create an icon manually by selecting **Connection → New Profile** (please see **Chapter 3: Raritan Remote Client (RRC), *RRC Navigator, Creating New Profiles*** for more information).
6. Double-click on the icon that corresponds to your Dominion KX unit.

Establish a Connection

When you double-click on your Dominion KX icon, its login screen appears. Log on with your username and password (default: **admin/raritan**) to connect to your Dominion KX unit. Use the RRC Navigator, on the left side of the RRC window, to select and connect to a server port.

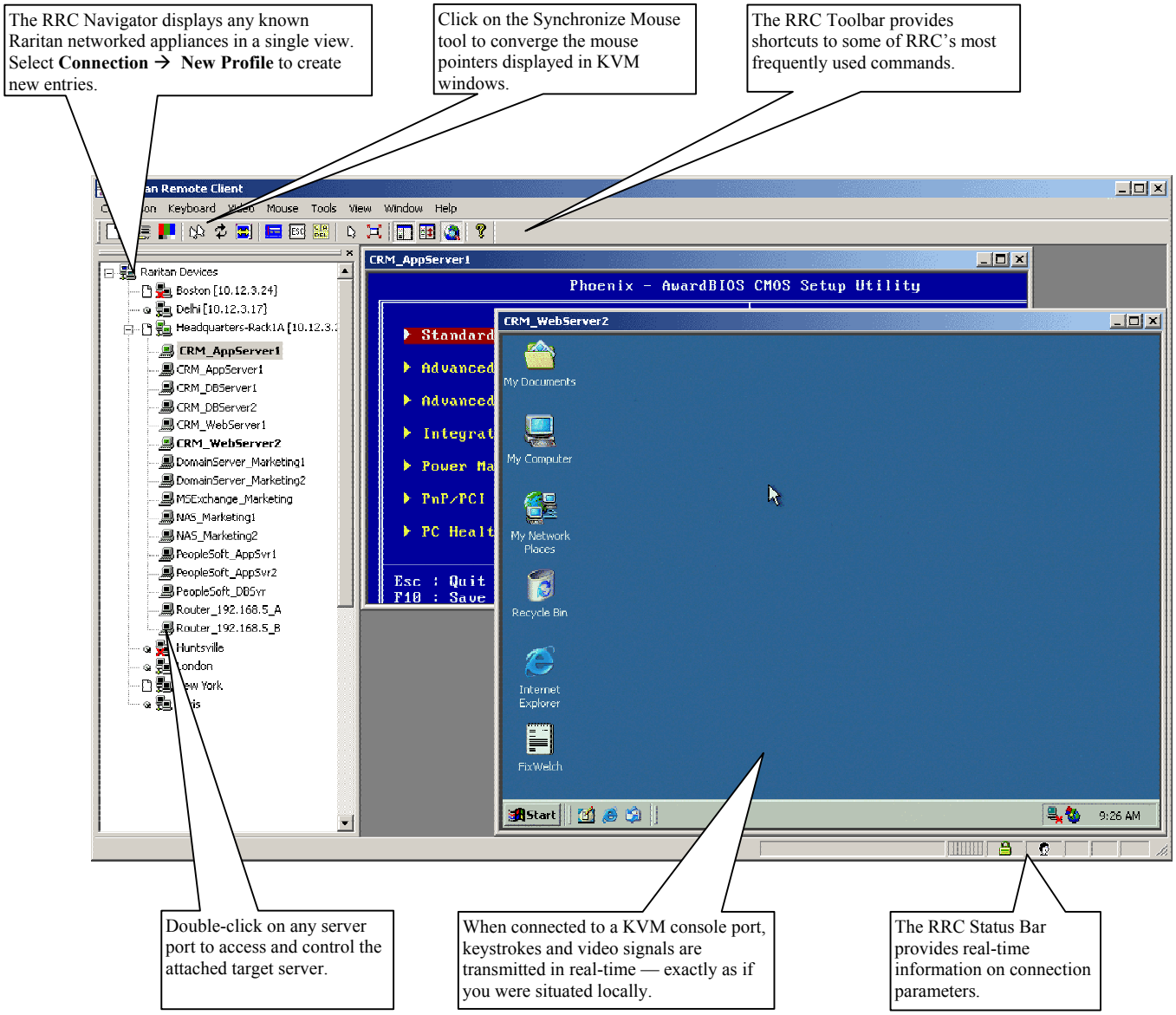
The RRC Navigator displays any known Raritan networked appliances in a single view. Select **Connection** → **New Profile** to create new entries.
Click on the Synchronize Mouse tool to converge the mouse pointers displayed in KVM windows.
The RRC Toolbar provides shortcuts to some of RRC's most frequently used commands.
Double-click on any server port to access and control the attached target server.
When connected to a KVM console port, keystrokes and video signals are transmitted in real-time — exactly as if you were situated locally.
The RRC Status Bar provides real-time information on connection parameters.

Figure 8 RRC Screen

Mouse Pointer Synchronization

When controlling a target server, RRC displays two mouse cursors: one cursor belongs to your client workstation and the other belongs to the target server. When properly configured, the two mouse cursors will align. Should you experience difficulty with mouse synchronization, please refer to the section **Configuring Target Servers**, at the beginning of this chapter.

Chapter 3: Raritan Remote Client (RRC)

Invoking RRC via Web Browser

Dominion KX features Web Browser access capabilities, providing a connection from any Windows-based Remote PC running Microsoft Internet Explorer 4.0+, Mozilla 1.1+, and Netscape 7+.

Security Settings

In order to access Dominion KX via web browser, your web browser must be configured appropriately, in particular, the Internet Explorer security settings tab:

- **Download Signed ActiveX controls** should be set to either "Enable" or "Prompt"
- **Run ActiveX controls and plug-ins** should be set to either "Enable" or "Prompt"

Please consult your Microsoft Internet Explorer documentation for details regarding these settings.

Note: *Microsoft Windows 2000, Microsoft Windows XP, and Microsoft Windows 2003 restrict certain types of users from downloading and running ActiveX controls and plug-ins, regardless of the above settings in Internet Explorer. Please consult your Microsoft Windows documentation for more information.*

Launching RRC

1. Ensure that your browser security settings are configured appropriately and type the IP address assigned to your Dominion KX unit (see **Chapter 2: Installation,** ***Initial Configuration***) in the URL/ Address text box of your web browser.

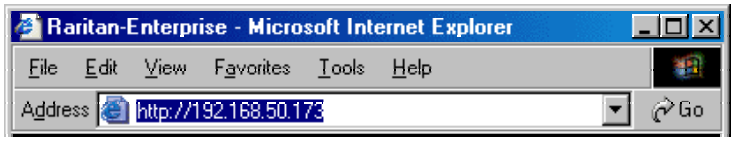

Figure 9 Type the IP Address of your Dominion KX unit

Note: *Dominion KX ships with the default IP address of 192.168.0.192*

2. Dominion KX will redirect you to an HTTPS (128-bit) secure web page for launching RRC.

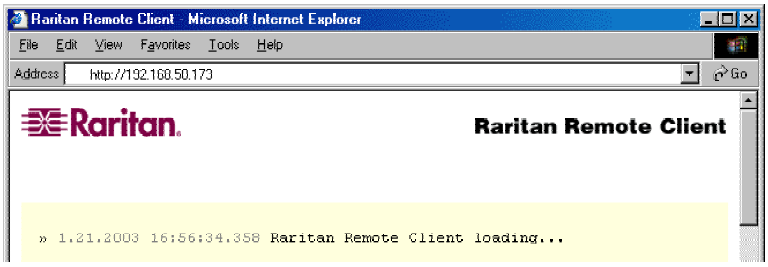

Figure 10 RRC Loading Screen

3. Depending on your browser's security configuration, you may see any or all of the following dialog boxes, confirming access and launch of an externally-provided program. Click [**Yes**] to advance through any of these prompts.

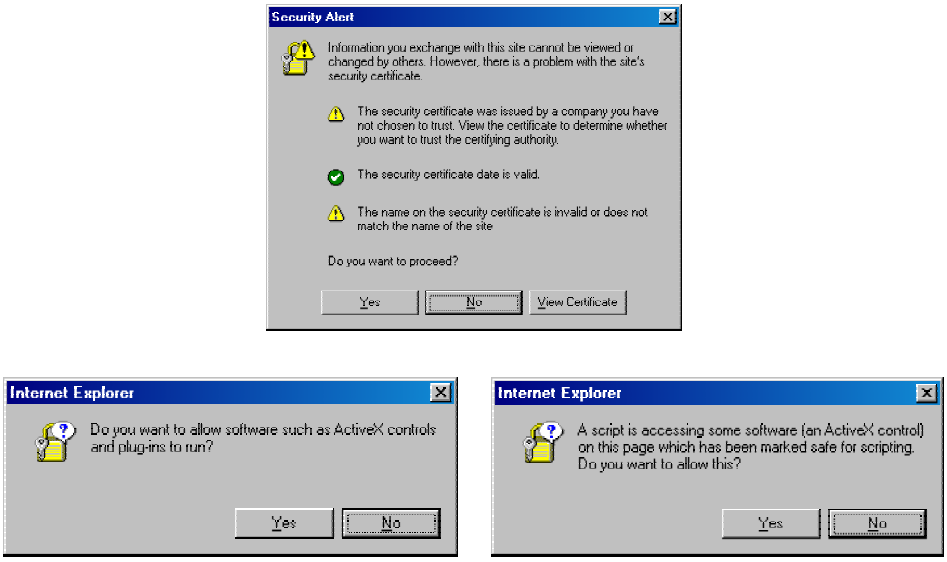
Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate
Internet Explorer
Do you want to allow software such as ActiveX controls and plug-ins to run?
Yes
No
Internet Explorer
A script is accessing some software (an ActiveX control) on this page which has been marked safe for scripting. Do you want to allow this?
Yes
No

Figure 11 Possible Security Alert Screens

Removing RRC From the Browser Cache

To remove RRC from your browser cache for any reason, follow the standard procedure as proscribed by your web browser software.

Directions for Internet Explorer v6.0:

1. If you have used RRC recently, exit and restart Internet Explorer.
2. On the Internet Explorer menu bar, select **Tools → Internet Options**.
3. When the **Internet Options** dialog box appears, click on the **Settings** tab.
4. When the **Settings** screen appears, click **View Objects**.
5. Internet Explorer will display a list of cached program objects. Select any entries named "TeleControl Class," "Raritan Console," or "Power Board" and delete them.

Optional: Installing RRC Software

Note: *This step is optional. Dominion KX can be accessed from a Remote PC either by installing RRC software, or by launching RRC via web browser (see previous section). Accessing Dominion KX via web browser does not require any software installation on the Remote PC. This section lists the steps required to invoke RRC using standalone software, which may be useful for accessing Dominion KX via modem or if you wish to close firewall access to ports 80 and/or 443.*

1. Insert the RRC CD-ROM (included) into the CD-ROM drive of your PC. Make sure the RRC version indicated is v4.0 or greater.
2. The RRC setup program will run automatically. If it does not, right-click on your PC's CD-ROM drive in Windows Explorer and choose **Auto Play**.
3. Follow the on-screen instructions given by the InstallShield Wizard to complete RRC installation on your Remote PC.
4. Depending upon the configuration of your PC, the RRC installation program may also automatically install DirectX and Microsoft Foundation Class libraries if required. If this happens, you will be asked to restart your PC after installation.
5. A Raritan Remote Client icon will be added to your desktop. Click on this icon to launch RRC.

RRC Window Layout

RRC functions are grouped into five general sections on the screen. Each section will be discussed in detail further in this chapter.

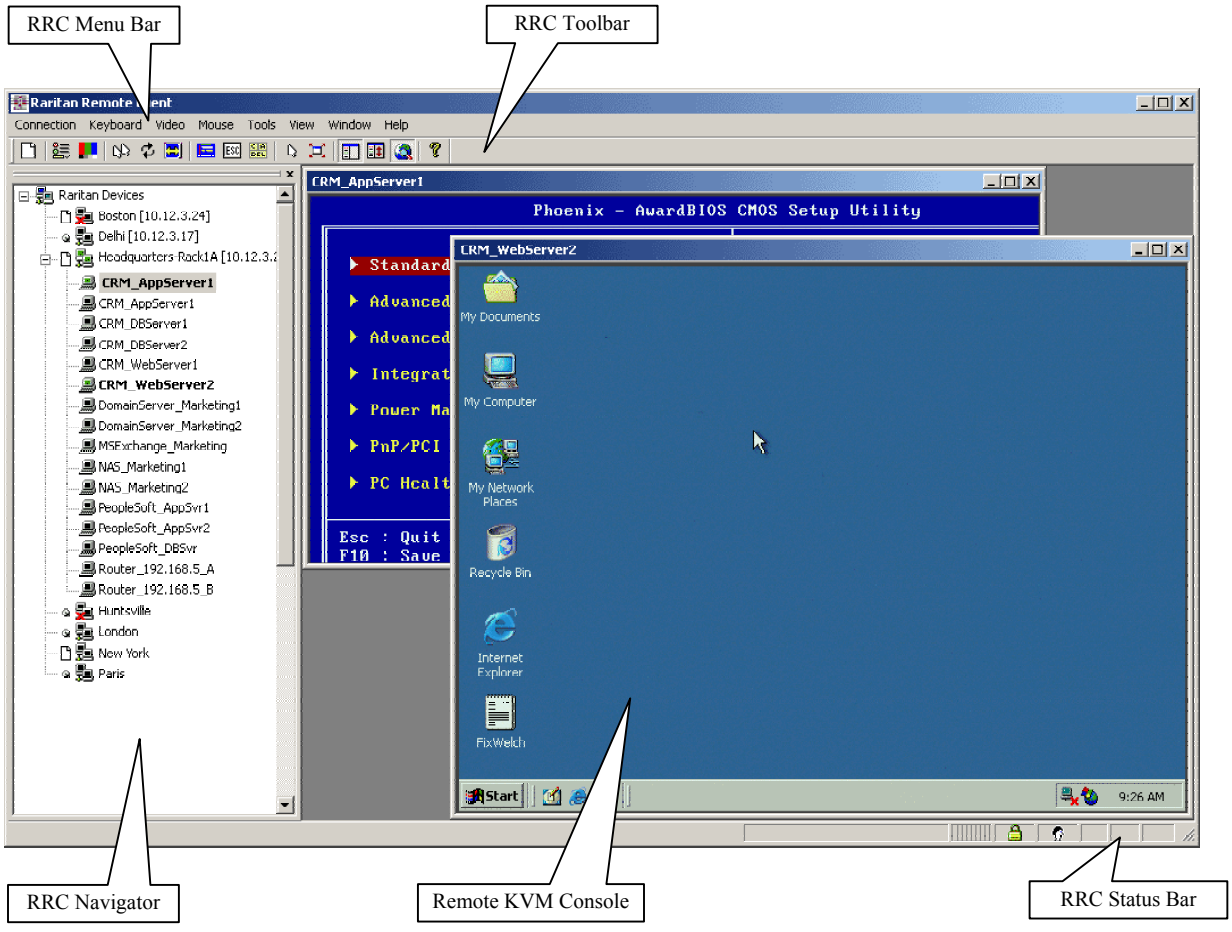

Figure 12 RRC Screen Components

RRC Navigator

The RRC Navigator provides a tree view of every known Raritan KVM Over IP device so you can access all Raritan networked appliances for which a connection profile exists. All Raritan devices automatically identified on the network are displayed.

Note: *Automatic Raritan device identification uses the UDP protocol, and will typically identify all Raritan devices on your subnet. Network administrators rarely allow UDP to function outside of a subnet. Automatic Raritan device identification will find only those Raritan devices that are configured to use the default TCP Port (5000).*

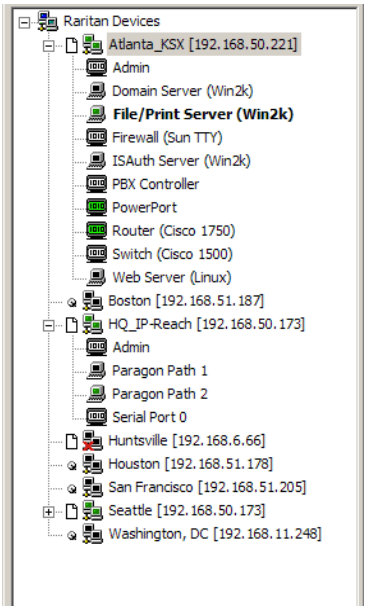

Figure 13 Expanded RRC Navigation Tree

Each device entry in the RRC Navigator provides two icons to communicate network status and connection profile information.

Left Icon (Connection Profile)

	Profiled – A network connection profile exists for this device.
	Modem Profile – A modem connection profile exists for this device.
	Not Profiled – RRC found this device on the network, but a connection profile does not exist for it.

Right Icon (Network Status)

	Connected (green) – You are currently authenticated and connected to this device.
	Available (black) – This device is currently available on the network, but you are not currently connected to it.
	Unavailable – A profile exists for this device, but it is not currently available on the network. (Note that all devices with modem profiles to which you are not currently connected will display this icon.)

For each Raritan device to which you are connected, RRC Navigator expands its display tree to show each port for which you have access.

- Ports displayed with a green icon indicate that you are connected to that port.
- Bold type indicates which port is currently displayed (active) in the remote desktop area of the client.

For each server port entry, RRC navigator displays the following icons:

	Connected (green)
	Available for connection
	Unavailable (no device connected, or access is blocked)
	Unavailable (in use by another [PC Share mode off])

Navigator Options

Certain RRC Navigator attributes may be customized to your preferences.

	Display / Hide Navigator – Toggle whether the RRC Navigator is shown. This option can also be toggled by choosing **View → Navigator** from the Menu Bar.
	Refresh Navigator – Update the device status information shown in the RRC Navigator.
	Show Browsed Devices – Toggle whether RRC Navigator should display "Not Profiled" devices automatically found on the network or show only devices for which profiles exist. This option can also be toggled by choosing **View → All Devices** from the Menu Bar.

***Note**: The Browse connection method is the only method of connecting to a Raritan Device configured to use DHCP IP addressing.*

Creating New Profiles

Connection profiles store important information about your Raritan device such as IP Address, custom TCP ports, preferred compression settings, and custom security keys.

***Note:** If your Raritan device is configured to use a custom TCP port (see **Chapter 4: Administrative Functions,** **Network Configuration**), or a group security key (see **Chapter 4: Administrative Functions,** **System-Level Security Parameters**), first create a connection profile so you can access the device.*

1. On the **Connection** menu, click **New Profile**. The **Connection Profile** dialog box appears, displaying all connection profiles which currently exist.

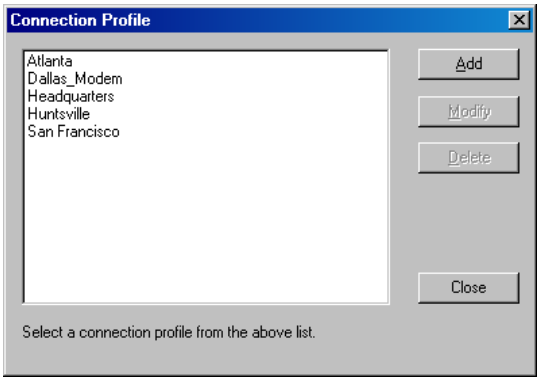

Figure 14 Connection Profile Window

2. Click [**Add**]. The **Add Connection** dialog appears. Options are grouped into three tabs.
   a. **Connect** tab

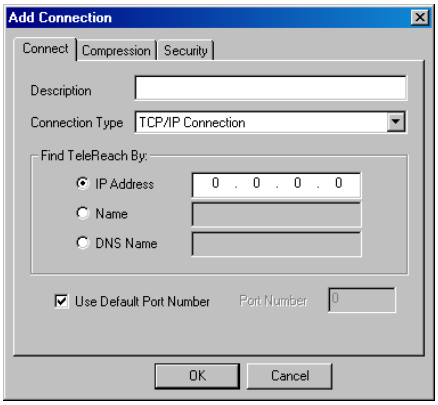

Figure 15 Connect tab

- **Description**: Type a text name that identifies the Raritan device you are configuring, such as "Atlanta_Datacenter."
- **Connection Type**: Select TCP/IP Connection for a LAN/WAN connection, or select Dial-Up Connection for a direct analog modem connection to the Raritan device.

For a **TCP/IP Connection**, select the option button before the method by which RRC should locate your Raritan device:

- **IP Address**: Type the IP address assigned to your Raritan device (see **Chapter 4: Administrative Functions, *Network Configuration***).
- **Name**: Type the name assigned to your Raritan device during initial setup (see **Chapter 4: Administrative Functions, *Network Configuration***).
- **DNS Name**: If you have configured your DNS server to resolve a DNS name to the IP address that you have assigned to your Raritan device, type the DNS name.

Note**: If using dynamic DHCP addressing, select to option button to Find Dominion KX **by Name.** The factory default unit name for each Dominion KX produced is **Dominion KX**. To change the default name on a Dominion KX unit and institute a unique name, please see **Chapter 4.

For a **Dial-Up Connection**, enter the dialing parameters that RRC should use to establish a connection:

- **Phone Number**: Be sure to include any additional codes that RRC should dial to establish a connection, such as country codes, area codes, or outside line access codes.
- **Modem**: Select the modem, as configured in Windows, that RRC should use to dial and connect to your Raritan device.

Select a TCP Port to use:

- **Use Default Port Number**: Dominion KX is configured by default to use TCP Port 5000 for communicating with RRC. Dominion KX can be configured to use a different TCP Port (**see Chapter 4: Administrative Functions, *Network Configuration***); if so, uncheck the **Use Default Port Number** option, and enter the configured TCP Port to be used.

   b. **Compression** tab
   Settings under the **Compression** tab are adjustable via the RRC client, and not necessary for pre-configuration in the Connection Profile. Should you wish to pre-configure these settings, however, refer to the section **Connection and Video Properties** in this chapter.

c. **Security** tab

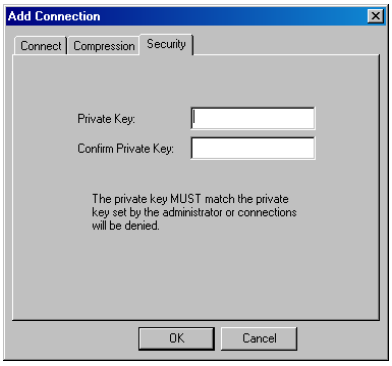

Figure 16 Security tab

If you have configured your Dominion KX unit to use a private security key (see **Chapter 4: Administrative Functions, *System-Level Security Parameters***), enter it here in order to be authorized to initiate a connection with that Dominion KX unit. Click [**OK**] when you have completed the fields.

When you have completed the **Connect** and **Security** tab screens, click [**OK**] create the connection.

Establishing a New Connection

Double-click the icon of a Raritan networked device in the RRC Navigator to connect, after entering your user name and password.

Note: *The default Dominion KX login user name is* ***admin****, with the password* ***raritan****. This user has administrative privileges. Passwords are case sensitive and must be entered in the exact case combination in which they were created. The default password* ***raritan*** *must be entered entirely in lowercase letters. To ensure security, change the default username password as soon as possible.*

If you do not see an icon for your Dominion KX in the RRC Navigator, please follow the instructions in the **Creating New Profiles** section in this chapter to create a new connection profile for your Dominion KX.

If you are having problems connecting to a Raritan device, be sure to check the following:

- **Username / Password**: Raritan usernames and passwords are case-sensitive.
- **TCP Port**: If you have configured your Raritan Device to use a non-default TCP Port, this information must be entered into its connection profile.
- **Firewall Settings**: If you are accessing a Raritan Device through a firewall, that firewall must be configured to allow two-way communication on TCP Port 5000 (or the custom TCP Port to which your Raritan Device has been configured).
- **Security Key**: If you have configured your Raritan Device to require a group security key, that key must be entered into the device's connection profile.

Closing a Remote Connection

To end your Dominion KX connection, right-click on the icon and select **Disconnect** from the menu.

RRC Toolbar and Shortcuts

The RRC Toolbar provides one-click access to the most frequently-used commands.

Figure 17 RRC Toolbar

BUTTON	BUTTON NAME	HOTKEY	FUNCTION
	New Profile	<Ctrl+Alt+C>	Creates a new Navigator entry for a Raritan device; same results as selecting **Connection → New Profile** in the menu bar.
	Connection Properties	<Ctrl+Alt+P>	Opens Modify Connection Properties dialog box to manually adjust bandwidth-correlated options (Connection Speed, Color Depth, etc.).
	Video Settings	N/A	Opens the Video Settings dialog box to manually adjust video conversion parameters.
	Synchronize Mouse	<Ctrl+Alt+S>	In dual-mouse mode, forces realignment of target server mouse pointer with Raritan Remote Client mouse pointer.
	Refresh Screen	<Ctrl+Alt+R>	Forces refresh of video screen.
	Auto-sense Video Settings	<Ctrl+Alt+A>	Forces refresh of video settings (resolution, refresh rate).
	Enter On-Screen Menu	N/A	Not applicable for Dominion KX. Used by RRC with other Raritan products.
	Exit On-Screen Menu	ESC	Not applicable for Dominion KX. Used by RRC with other Raritan products.
	Send Ctrl+Alt+Del	<Ctrl+Alt+D>	Sends a Ctrl+Alt+Del key sequence to the target server.
	Single Cursor Mode	<Ctrl+Alt+X>	Enters Single Cursor Mode, in which the local PC's mouse pointer no longer appears on-screen. Press <Ctrl+Alt+X> to exit this mode.
	Full Screen Mode	<Ctrl+Alt+F>	Maximizes the screen real estate to view the target server desktop.
	Show / Hide Navigator	N/A	Toggles whether or not the RRC Navigator is displayed.
	Refresh Navigator	N/A	Forces a refresh of the data displayed by the RRC Navigator.
	Show / Hide "Browsed" Devices	N/A	Toggles whether or not the RRC Navigator displays Raritan Devices automatically identified on the network (that do not have pre-configured profiles associated with them).
	About	N/A	Displays version information about Raritan Remote Client.

RRC Status Bar

The RRC Status Bar displays session information about your connection to your Dominion KX.

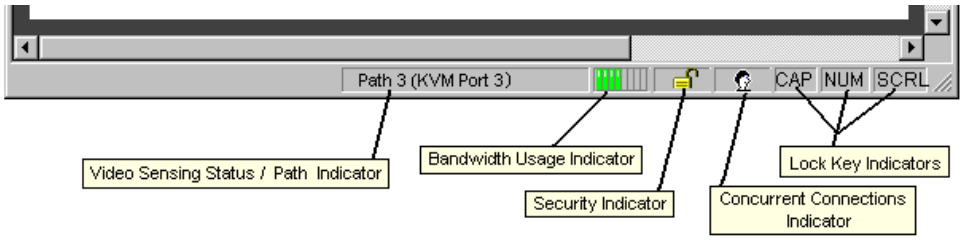

Figure 18 RRC Status Bar Components

- **Video Sensing Status / Path Indicator**: indicates the occurrence of video sensing, during connections to target KVM Server ports.
- **Bandwidth Usage Indicator**: indicates how much of your total available bandwidth is currently being used. The **Connection Speed** setting, found under the Compression tab of the Connection Properties screen, determines total available bandwidth.
- **Security Indicator**: indicates whether the current remote connection is protected by encryption. Encryption requirements are set during Dominion KX configuration (see **Chapter 4**). When a Dominion KX device is configured for **No encryption** or **SSL Authentication, NO data encryption**, the Security Indicator is represented on the Status Bar as an open lock. When **SSL authentication, data encryption** or **SSL authentication, SSL encryption** is selected, the Security Indicator is represented on the Status Bar as a closed lock.
- **Concurrent Connections Indicator**: indicates if multiple remote users are currently connected to the same Dominion KX target server, showing one icon for a single connected user, and two icons if two or more users are connected.
  Concurrent connection ability can be set globally under **PC Share Mode** on the Security Configuration screen (see **Chapter 4**), or set per individual user in the **Concurrent Access Mode** setting on the User Account Settings screen (see **Chapter 4**).
- **Lock Key Indicators**: indicates the status of the current target KVM Server, with respect to the activation of the Caps-Lock, Num-Lock, and Scroll-Lock keys. If these keys are enabled on the target server being viewed, this affirmative status will be reflected on the Status Bar as indicated.

Remote KVM Console Control

Once you establish a connection with a Dominion KX unit, that unit's icon in the RRC Navigator expands to display all ports enabled for remote access.

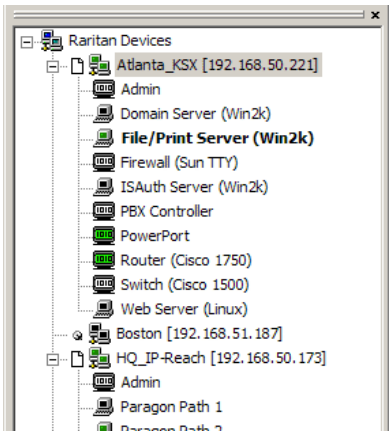

Figure 19 Navigation Tree

To establish a remote KVM console connection, double-click on the KVM port you want to control. Once connected, Dominion KX displays real-time video output by the target server that is connected to your Dominion KX KVM port. This video is compressed and encrypted according to the configuration settings specified by the Administrator (please see **Chapter 4**). You now have complete, low-level control of the KVM console as if you were physically located next to the server.

Single Mouse Mode / Dual Mouse Mode

When remotely viewing a target server that uses a pointing device, you will see two mouse pointers in the Remote Desktop. When your mouse pointer lies within the Remote Desktop area of RRC, mouse movements and clicks are directly transmitted to the target server connected. RRC's mouse pointer, generated by the operating system on which RRC is running, slightly leads the target server's mouse pointer during movement, a necessary result of digital delay.

On fast LAN connections, some users disable the RRC mouse pointer and view only the target server's mouse pointer. To toggle between these two modes, use the <**Ctrl+Alt+X**> hotkey, or press the **Single Mouse Pointer** mode icon in the RRC Toolbar.

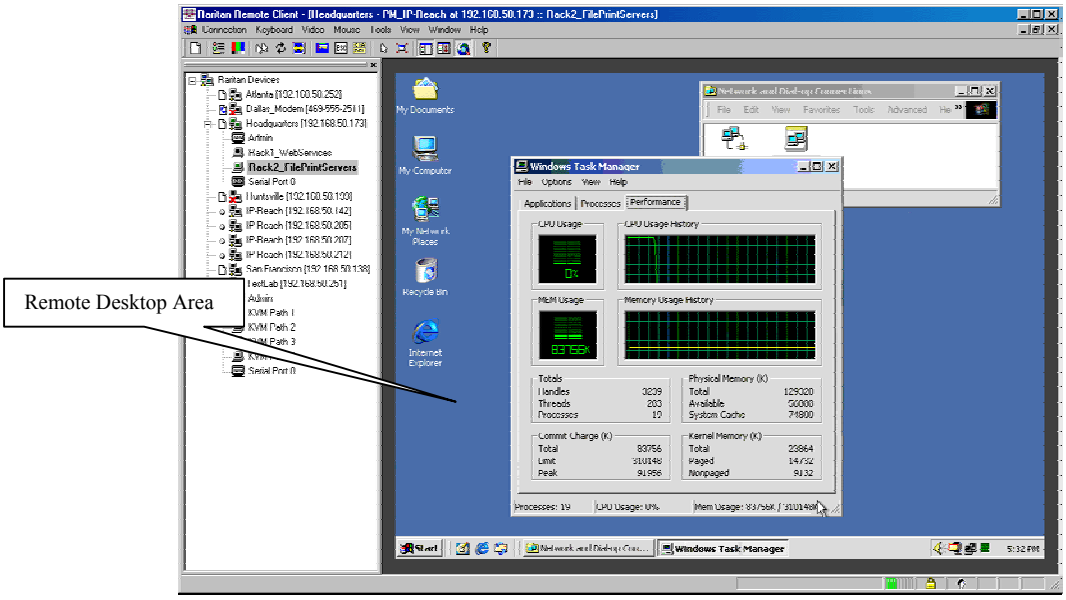

Figure 20 Remote Desktop, where dual mouse cursors will appear

For better alignment of mouse pointers, click on the **Synchronize Mouse** shortcut on the RRC Toolbar, or simultaneously press the keys <**Ctrl+Alt+S**>. This forces the realignment of the mouse pointers. If you have carefully followed **Chapter 2: Installation, Configuring Target Servers** and the mouse pointers remain out of sync, click on the [**Auto-Sense Video**] button on the RRC Toolbar.

Full Screen Mode

RRC's Full Screen mode removes window borders, toolbars, status bars, and the RRC Navigator to maximize screen space. This is useful when viewing a target KVM Server whose video resolution is equal to or greater than the video resolution setting of the PC on which RRC is running, for example, viewing a 1028x768 server on a 1028x768 PC.

To toggle Full Screen Mode, click on the **Full Screen Mode** shortcut on the RRC Toolbar (or press the hotkey combination <**Ctrl+Alt+F**>).

To exit Full Screen Mode, press the hotkey combination <**Ctrl+Alt+F**>.

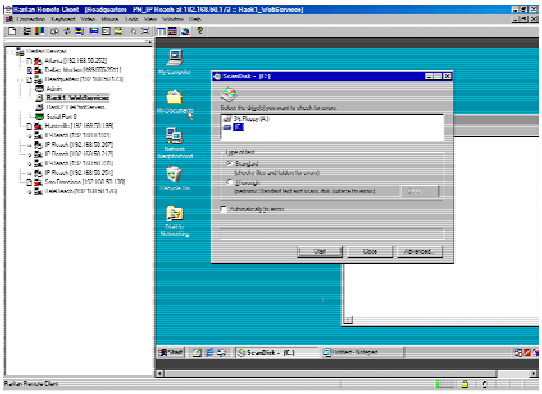

Figure 21 Standard View

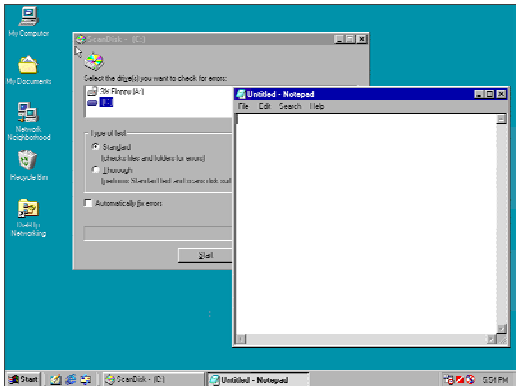

Figure 22 Full Screen Mode

Keyboard Macros

Dominion KX's Keyboard Macro feature ensures that keystroke combinations intended for the target server are sent to, and interpreted only by, the target server. Otherwise, they might be interpreted by the computer on which RRC is running.

Ctrl+Alt+Delete Macro

Due to its frequent use, a Ctrl+Alt+Delete macro has been pre-programmed into RRC.

	Send Ctrl+Alt+Del	<Ctrl+Alt+D>	Sends a Ctrl+Alt+Delete macro to the target server.

Clicking on the **Ctrl+Alt+Delete** shortcut in the RRC Toolbar sends this key sequence to the server or KVM switch to which you are currently connected. In contrast, if you were to physically press the Ctrl+Alt+Delete keys while using RRC, the command would first be intercepted by your own PC due to the structure of the Windows operating system, instead of sending the key sequence to the target server as intended.

Building a Keyboard Macro

These directions describe how to create a keyboard macro for the Windows command Minimize **All Windows/Show Desktop**. Follow these steps, substituting the appropriate key combination for the command you want, to create your own macro.

Example: In Windows, pressing the <**Windows+D**> key combination minimizes all program windows. However, when connected to a target server with RRC, a keyboard macro is the only means to accomplish this task on the target server – because, again, pressing the key combination <**Windows+D**> would result in your own client PC intercepting the command and performing it – instead of sending the command to the target server as intended.

1. On the **Keyboard** menu, click **Keyboard Macros**.
2. When the **Keyboard Macros** window appears, click [**Add**] to add a new macro. The **Add Keyboard Macro** window appears.

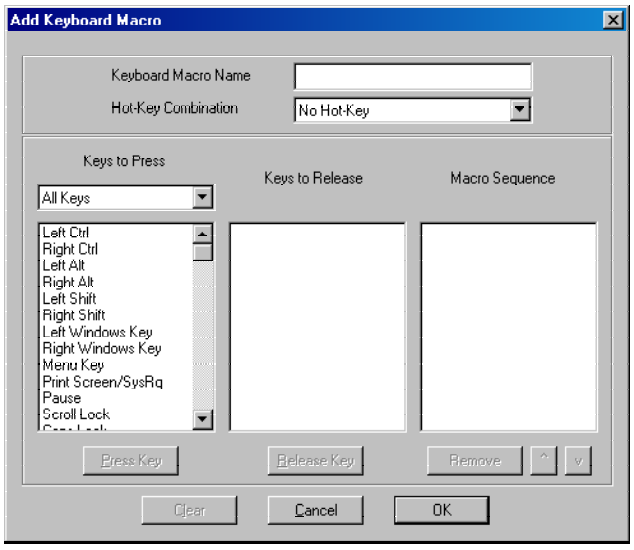

Figure 23 Add Keyboard Macro Window

3. Build the Keyboard Macro by editing the fields in the **Add Keyboard Macro** window:
   a) Type a name in the **Keyboard Macro Name** field. This name will appear on the RRC Menu Bar after the macro is created. In this example, type **Minimize All Windows**.
   b) **Optional**: In the **Hot-Key Combination** field, type a keyboard combination. This allows you to execute the macro from your keyboard when RRC is running. *In this example*, press the <**Ctrl**> <**Alt**> and number <**1**> keys (<**Ctrl+Alt+1**>).

c) In the **Keys to Press** drop-down list, select each key for which you would like to emulate key presses – in the order by which they are to be pressed. Click [**Press Key**] after each selection. As each key is selected, it will appear in the **Keys to Release** field. *In this example*, select two keys: the <**Windows**> key and the letter <**D**> key.

d) In the **Keys to Release** field, select each key for which you would like to emulate key releases – in the order by which they are to be released. Click [**Release Key**] after each selection. *In this example*, both keys pressed must also be released.

e) Review the **Macro Sequence** field – the contents are automatically generated depending on the **Keys to Press** and **Keys to Release** selections. Ensure that the contents list the exact key sequence you want. To remove a step in the sequence, select it, and click [**Remove**]. To change the order of steps in the sequence, select the step and click [↑] and [↓] to re-order the steps.

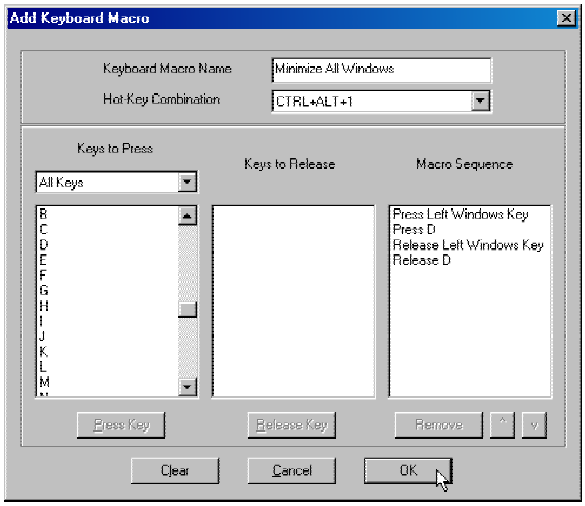

Figure 24 Add Keyboard Macro Window

4. Click [**OK**] to save the macro, or [**Cancel**] to close the window without saving. Click [**Clear**] to clear all field and start over. When you click [**OK**], the **Keyboard Macros** window appears, listing the new keyboard macro.

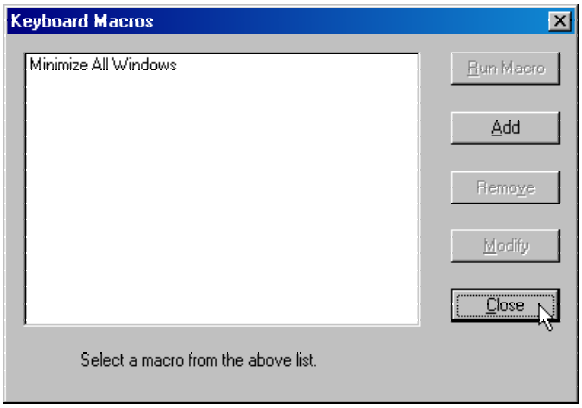

Figure 25 Keyboard Macros Window

5. Click [**Close**] to close the window.

Running a Keyboard Macro

Once you have created a keyboard macro, execute it from the RRC Menu Bar, or by using the hotkey (keyboard) combination if you assigned one while creating the macro.

Menu Bar Activation

When you create a macro, it appears under the **Keyboard** menu. From the **Keyboard** menu, click on the name of your keyboard macro.

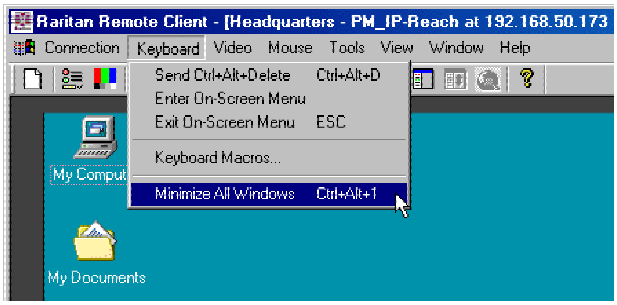

Figure 26 Minimize All Window Menu Option

Hot-Key Activation

When you create a macro, execute it in RRC by pressing the hotkey you assigned to it. *In this example*, press the keys <**Ctrl+Alt+1**> simultaneously to send the Minimize All Windows combination <**Windows+D**> to the target server.

Connection and Video Properties

Dominion KX's dynamic video compression algorithms maintain KVM console usability under varying bandwidth constraints. Dominion KX is unique in that it optimizes its KVM output for not only LAN utilization, but also via the WAN and dial-up. It also adjusts color depth and can limit video output, offering an optimal balance between video quality and system responsiveness in any bandwidth constraint.

Power users of RRC should understand the following adjustable parameters in the **Connection Properties** and **Video Settings** dialog boxes, and familiarize themselves with the effects of each setting – in different operating environments, they can be optimized to your requirements.

Connection Properties

	Connection Properties	<Ctrl+Alt+P>	Opens Modify Connection Properties dialog box to manually adjust bandwidth-correlated options (Connection Speed, Color Depth, etc.).

1. On the **Connection** menu, click **Connection Properties.** The **Modify Connection** window appears.

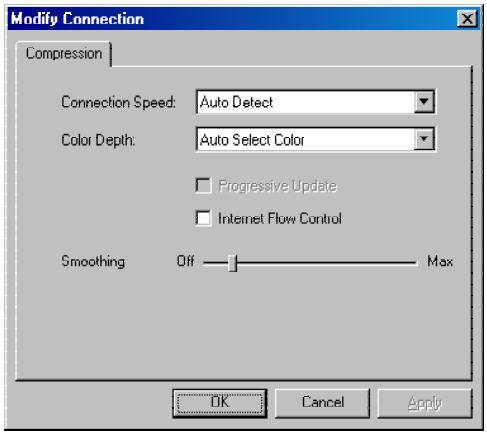

Figure 27 Modify Connection Window

- **Connection Speed:** Use the **Connection Speed** setting to manually tell Dominion KX of bandwidth constraints. Dominion KX can adapts its speed and not use more than the bandwidth that is available. Dominion KX detects available bandwidth automatically, but you can adjust this use.
- **Color Depth:** Dominion KX can dynamically adapt the color depth transmitted to remote users in order to maximize usability in all bandwidth constraints.
  - **Progressive Update** option**:** Progressive Update can increase usability in constrained bandwidth environments. When **Progressive Update** is enabled, Dominion KX first sends an image of the remote desktop at lower color depths, and then provides higher color depth images as bandwidth allows.

Important: For most administrative tasks (server monitoring, reconfiguring, etc.), server administrators do not require the full 24-bit or 32-bit color spectrum made available by most modern video graphics cards. Attempting to transmit such high color depths, then, would waste an enormous amount of precious network bandwidth.

Note: *When Color Depth is set to* ***Auto Select Color*** *(default),* ***Progressive Update*** *is automated. Dominion KX will enable/disable Progressive Update as needed, disabling it for fast connections and enabling it for slow connections.*

- **Internet Flow Control:** When using Dominion KX over an unpredictable public WAN (particularly in international scenarios), checking the **Internet Flow Control** check box ensures that packets transmitted by Dominion KX are received and reconstructed by RRC in the correct order.

- **Smoothing**: The video **Smoothing** level you set instructs Dominion KX to what degree color gradation shifts are relevant for transmission. Video pixels that stray from the majority color are assigned approximated color values to reduce bandwidth used and video noise transmitted. Overly high smoothing levels can result in color inaccuracies; whereas lower smoothing levels require greater bandwidth and processing power.

2. Click [**OK**] to set Connection Properties or [**Cancel**] to close the window without saving changes.

Video Settings

	Video Settings	N/A	Opens the Video Settings dialog box to manually adjust video conversion parameters.

1. On the **Video** menu, click **Video Settings**. The **Settings** window appears.

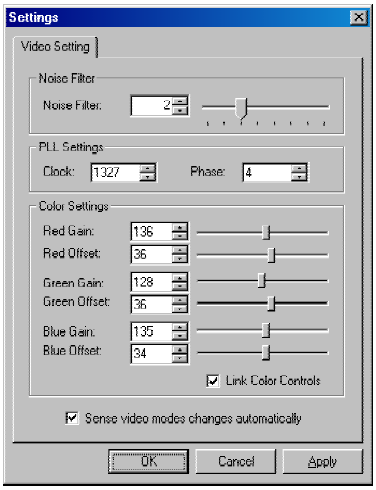

Figure 28 Settings Window

Most settings here are refreshed by performing a Color Calibration (described in the next section), or by manually forcing Dominion KX to auto-detect the video settings (on the **Video** menu, click **Auto-sense Video Settings**). However, it is useful to understand the settings.

- **Noise Filter:** Dominion KX can filter out electrical interference of video output from graphics cards. This feature optimizes picture quality and reduced used bandwidth.
  - *Higher:* Noise Filter settings instruct Dominion KX to transmit a variant pixel of video only if a large color variation exists in comparison to its neighbors. However, setting the threshold too high can result in the unintentional filtering of desired screen changes.
  - *Lower:* Noise Filter settings instruct Dominion KX to transmit most pixel changes. Setting this threshold too low can result in higher bandwidth use.

Note: *Lower Noise Filter settings (approximately 1 to 4) are recommended. Although higher settings will stop the needless transmission of false color variations, true and intentional small changes to a video image may not be transmitted.*

- **Analog-to-Digital Settings:** The following parameters are best left to Dominion KX to automatically detect (on the RRC Menu Bar, select **Video > Auto-sense Video Settings**), but a brief description of each is included here.
- **PLL Settings**: If the video image looks extremely blurry or unfocused, the PLL Settings for clock and phase can be adjusted until a better image appears on the active target server.
  - **Clock:** Horizontal sync divider to produce pixel clock. Controls how quickly video pixels are displayed across the video screen. Changes made to clock settings cause the video image to stretch or shrink horizontally. Odd number settings are recommended.
  - **Phase:** Phase values range from 0 to 31 and will wrap around. Stop at the phase value that results in the best video image for the active target server.

- **Color Settings:** Gain control can be thought of as contrast adjustment. Offset control can be thought of as brightness adjustment.
  - **Red Gain:** Controls the amplification of the red signal.
  - **Red Offset:** Controls the bias of the red signal.
  - **Green Gain:** Controls the amplification of the green signal.
  - **Green Offset:** Controls the bias of the green signal.
  - **Blue Gain:** Controls the amplification of the blue signal.
  - **Blue Offset:** Controls the bias of the blue signal.
  - **Link Color Controls:** Makes all the gain slide adjusters move in unison when any one color's gain slide is moved and all the offset slide adjusters move in unison when any one color's offset slide is moved.
- **Sense video mode changes automatically:** Determines whether Dominion KX will automatically update the video image being sent RRC each time it detects a change in video resolution or refresh rates at the target server.

2. Click [**OK**] to set Video Settings or [**Cancel**] to close the window without saving changes.

Color Calibration

Automatic Color Calibration adjusts the color settings on Dominion KX to reduce excess color noise and data during digitization of video images, increasing the performance of Dominion KX. Use the Color Calibration command if the color levels (hue, brightness, saturation) of transmitted video images do not seem accurate. Dominion KX color settings remain the same when switching from one target KVM Server to another, so you can perform Color Calibration once to affect all connected target servers.

1. Open a remote KVM connection to any server running a graphical user interface.
2. Ensure that a solid white color covers approximately 15% or more of the target server's desktop (suggestion: open Microsoft Notepad and maximize the window).

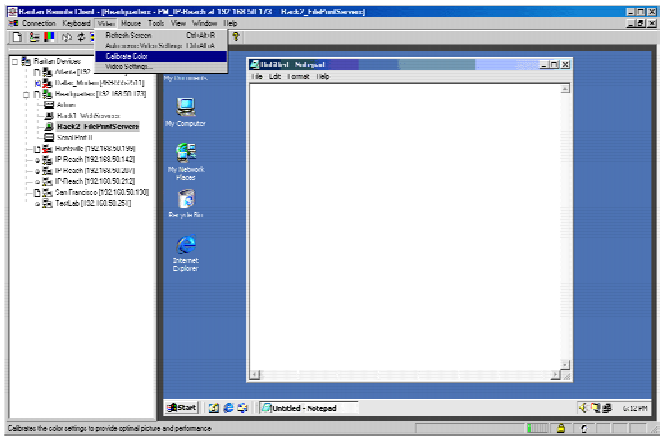

Figure 29 Example of Sizing the Notepad Window

3. On the **Video** menu, click **Calibrate Color**.

Select Administrative Functions via RRC

Although Dominion KX provides a remote interface to administrative functions through Dominion KX Manager, RRC provides an interface to frequently-used administrative functions directly from the RRC interface. When logged into a Dominion KX unit as an Administrator, you can perform the following administrative tasks directly from RRC.

Firmware Upgrade

On the **Tools** menu, click **Update Device** to perform firmware upgrades.

RRC will prompt you to locate a Raritan firmware distribution file (*.RFP format), found on the Raritan web site (www.raritan.com) when available. Be sure to read all instructions included in firmware distributions before performing an upgrade.

Device Restart

Select a device in the RRC Navigator, and on the **Tools** menu, click **Restart Device** to restart the Dominion KX unit.

Device Configuration Backup and Restore

On the **Tools** menu, click **Save Device Configuration** to download complete Dominion KX configuration to your local computer.

On the **Tools** menu, click **Restore Device Configuration** to upload the archived Dominion KX configuration.

Log Files

On the **Tools** menu, click **Save Activity Log** to download a detailed activity log for troubleshooting purposes.

On the **Tools** menu, click **Save Diagnostic Log** to download a detailed diagnostic log for viewing, reporting, and analysis.

Chapter 4: Administrative Functions

Launching Dominion KX Manager

After you assign an IP Address to your Dominion KX unit, all administrative functions can be performed remotely via Web browser using Dominion KX Manager.

Log on to a workstation with network connectivity to Dominion KX. Ensure this workstation has Java Runtime Environment (JRE) version 1.4.x or higher (download Java Runtime Environment at http://java.sun.com/).

Launch a web browser and access the URL **http://IP-ADDRESS/admin**, where **IP-ADDRESS** is the IP Address assigned to your Dominion KX unit (factory default: **192.168.0.192**). Your browser will prompt you to grant permission to retrieve and launch Dominion KX Manager, a signed Java applet. After you grant permission, Dominion KX Manager launches automatically.

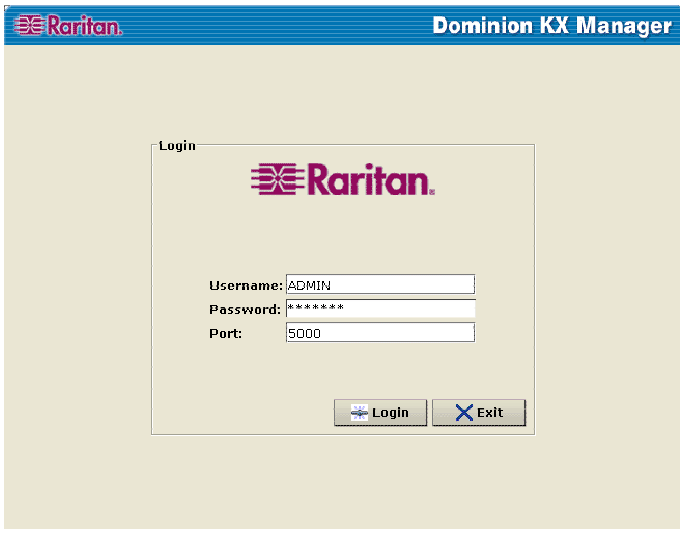

Figure 30 Dominion KX Manager Login Screen

Username / Password: Log on to Dominion KX Manager with the username and password of any user with Administrative privileges.

Note: *The default Dominion KX login user name is* ***admin*** *with the password* ***raritan;*** *this user has administrative privileges. Passwords are case sensitive and must be entered in the exact case combination in which they were created. The default password* ***raritan*** *must be entered entirely in lowercase letters. To ensure security, change the default username password as soon as possible.*

Port: If your Dominion KX unit has been configured to use a different TCP port than the default port 5000, enter the port number here.

Dominion KX Manager Interface

Dominion KX Manager provides an interface for performing configuration and administrative functions. Many of the commands available on the menu bar can be accessed by right-clicking on objects in the server and user lists on the left side of the screen.

Network Configuration

Use these descriptions to customize the network configuration settings of your Dominion KX unit such as IP Address, Ethernet speed, and other settings.

Important: Dominion KX must be rebooted before Network Configuration changes take effect.

1. On the **Setup** menu, click **Configuration**, and then click **Network**. The **Network Configuration** window appears.

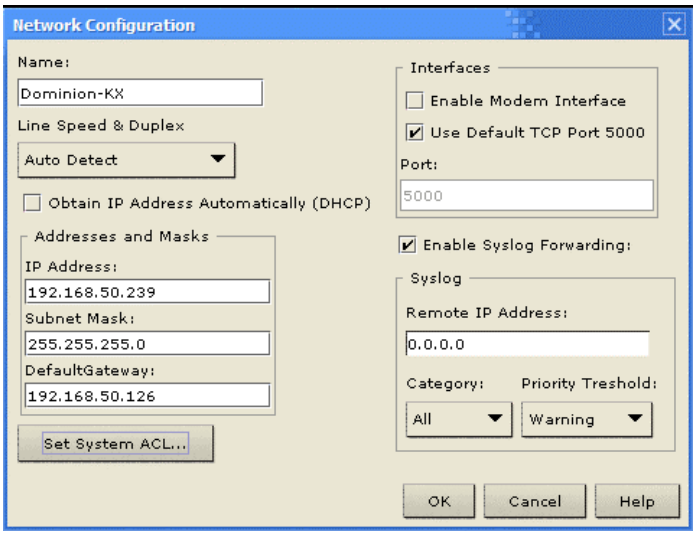

Figure 31 Network Configuration Window

You have seen most of these settings in networked devices, with the possible exception of the following parameters:

- **Name:** Type a unique name for the Dominion KX unit. The default name is **Dominion-KX**. Remote users will see and use this name to identify this particular Dominion KX unit.
- **Use Default TCP Port 5000**: Besides the initial download of Raritan Remote Client and Dominion KX Manager (which occurs over secure HTTPS Port 443), all communication to and from Dominion KX occurs over a single, configurable TCP Port. By default, this is set to Port 5000, but you may configure it to use any TCP port of your choice, except 80 and 443.

***Note:** In order to access Dominion KX from beyond a firewall, your firewall settings must enable two-way communication through the default port 5000 or the non-default port configured above.*

- **Enable Syslog Forwarding**: Click on this check box to send Dominion KX log messages to a remote syslog server. Type the IP Address of your syslog server in the **Remote IP Address** field, and click on the **Category** and **Priority Threshold** drop-down arrows to select the level of event sensitivity.

– **Set System ACL**: Click on this button to set a global-level access control list for Dominion KX, enhancing security by ensuring that Dominion KX does not respond to packets being sent from disallowed IP addresses. The **Access Control List** window appears.

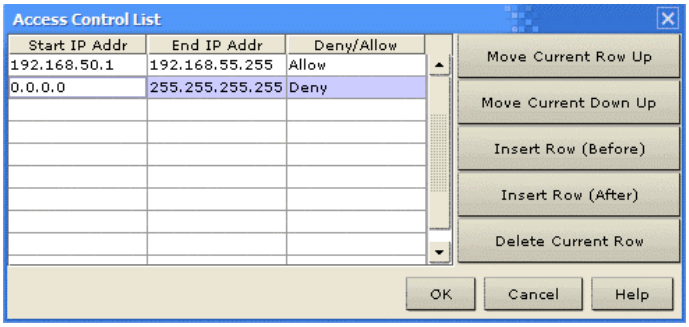

Figure 32 Access Control List Window

These ACL values are global, affecting the Dominion KX unit as a whole. Dominion KX allows you to create ACLs for each user group, for example, you can create a user group "Outsourced Vendors," that is permitted to access Dominion KX only from a given IP address range (please see the section **Users and Groups** in this chapter, for more information on how to create group-specific ACLs).

Important: Please note that ACL rules are evaluated in the order in which they are listed. For instance, if in the above example, the two ACL rules were reversed, Dominion KX would accept no communication at all. Use the buttons on the right of the window to adjust the order of your list.

2. Click [**OK**] to accept the Access Control List changes or [**Cancel**] to close the window without saving changes.
3. Click [**OK**] to set Network Configurations or [**Cancel**] to close the window without saving changes.

Reset Settings to Default

To delete all configured Dominion KX network settings and return to factory default settings, use the **Local Console Port** to reset all network settings (please see **Chapter 5: Local Console Port Access** for more information).

System-Level Security Parameters

Use these descriptions to change system-level security settings of your Dominion KX unit such as encryption levels, idle time, share mode, and other parameters.

Important: Dominion KX must be rebooted before Network Configuration changes take effect.

1. On the **Setup** menu, click **Security**, and then click **Configuration**. The **Security Configuration** window appears.

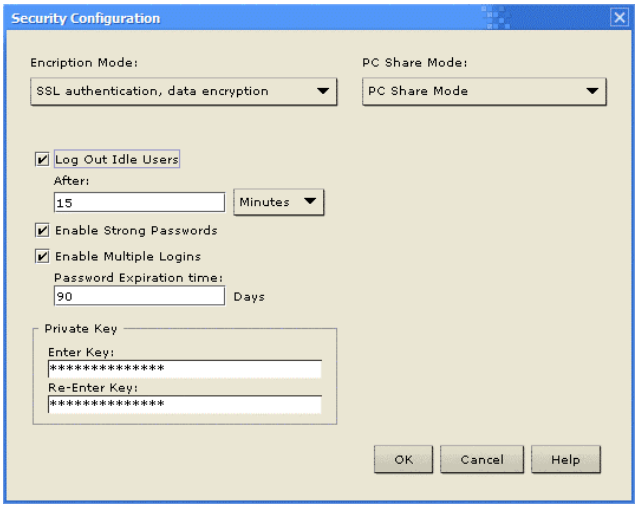

Figure 33 Security Configuration Window

– **Encryption mode** – click on the drop-down arrow to select one of the following:
  - **No encryption**: No data encryption applied to network transmissions. Not recommended except for closed Ethernet networks.
  - **SSL authentication, NO data encryption:** Usernames and passwords are secured, but KVM transmissions are not. 128-bit Secure Socket Layer (SSL) protocol provides a private communications channel between Dominion KX and the Remote PC during initial connection authentication. No encryption security in place during remote KVM data transfer.
  - **SSL authentication, data encryption:** Secures user names, passwords and KVM data, including video transmissions. 128-bit Secure Sockets Layer (SSL) protocol provides a private communications channel between Dominion KX and the Remote PC during initial connection authentication. After authentication, KVM data is also transferred with 128-bit encryption, but using a protocol much more efficient than SSL (RC4 encryption, but without SSL headers). Raritan recommends this option.
  - **SSL authentication, SSL data encryption:** Secures user names and passwords, and provides high-level security for KVM data. 128-bit Secure Sockets Layer (SSL) protocol provides a private communications channel between Dominion KX and the Remote PC during initial connection authentication. 128-bit SSL encryption is also in place during remote KVM data transfer. Note that because the SSL protocol was not designed for KVM communication, this mode is less efficient but no more secure than the recommended setting, above.

– **PC Share Mode** – Determines global concurrent remote access, enabling up to eight remote users to simultaneously log on to one Dominion KX unit and concurrently view and control the same target server through Dominion KX. Click on the drop-down arrow to select one of the following:
  - **Private Mode (default):** No PC Share. Each target server can be accessed exclusively by only one user at a time.

- **PC Share Mode:** Target servers can be accessed by more than one user (administrator or non-administrator) at a time. Control is based on first active keyboard/mouse input, so multiple remote users attempting keyboard input or mouse movement at exactly the same moment may experience uneven control.

Note: *PC Share Mode is a global setting. For individual user access settings see* ***Keyboard and Mouse Control*** *and* ***Concurrent Access Mode*** *on the* ***User Account Settings*** *screen. Each user profile can be set individually to enable/disable keyboard and mouse control, and concurrent access.*

- **PC Share Admins Only:** Target servers can be accessed by more than one user (administrative users only) at a time. Control is based on first active keyboard/mouse input, so multiple remote users attempting keyboard input or mouse movement at exactly the same moment may experience uneven control.

– **Log Out Idle Users:** Click on the check box to automatically disconnect remote users after a certain amount of inactive time has passed. Type the amount of time in the **After** field.

– **Enable Strong Passwords:** Requires user passwords to have a minimum of 6 characters with at least one alphabetical character and one non-alphabetical character (punctuation or number). The first four characters of the password and the username cannot match.

Note: *Strong password rules affect only those usernames and passwords stored by Dominion KX. If you configure Dominion KX to authenticate to a remote server such as LDAP, RADIUS, or Active Directory, these rules are not enforced by Dominion KX (please see the section* ***Remote Authentication*** *in this chapter for more information on remote authentication).*

– **Enable Multiple Logins:** When this rule is selected, a given username/password combination can be connected into Dominion KX from multiple client workstations at a time. Otherwise, such usage as disallowed.

– **Password Expiration Time:** Type a number of days in this field to force users to change their passwords after a set duration.

– **Private Key**: Type a private key password. Only those remote users who know the private key, in addition to their own usernames and passwords, can log in and connect to Dominion KX.

- **Re-Enter Private key:** Type private key password again for confirmation.

Note: *Private Key passwords are case sensitive. For remote user login, passwords must be entered by the user in the exact case combination in which they were created here. Please remember that private key passwords must be alphanumeric; special characters cannot be used.*

---

2. Click [**OK**] to set Security Configurations or [**Cancel**] to close the window without saving changes.

Users, Groups, and Access Permissions

Overview

Dominion KX keeps an internal list of user and group names to determine access authorization and permissions. This information is stored internally in a hashed / encrypted format.

Note to CommandCenter Users

If you plan to configure Dominion KX to be integrated with and controlled by Raritan's CommandCenter management appliance, this section of the User Manual does not apply to you. When a Dominion KX unit is controlled by CommandCenter, CommandCenter determines the allowed users and groups. Please refer to your CommandCenter User Guide.

Note to Raritan Customers Upgrading from Previous Firmware Versions

If you previously configured Raritan products such as Dominion KSX and IP-Reach running legacy firmware versions earlier than v3.2, read this entire section carefully. Beginning with firmware version v3.2 and above, the implementation of users and groups has changed significantly to provide more flexible and powerful configurations.

Relationship Between Users and Group Entries

You may want to organize the users in Dominion KX into groups. Assigning users to groups allows you to manage permissions for all users in a group at once, instead of managing permissions on a user-by-user basis.

User information is helps in authenticating users accessing Dominion KX. Upon successful authentication, Dominion KX uses **Group information** to determine the user's permissions – which server ports are accessible, whether rebooting Dominion KX is allowed, and other features.

You may choose not to associate specific users with groups. In this case, Dominion KX classifies the user as "**Individual**."

Mandatory User Groups

Every Dominion KX has three default user groups. These groups cannot be deleted:

ADMIN	User group for original, factory-default administrative user.
NONE	Permissions defined for this group are employed for a user when your Dominion KX is configured for remote authentication via LDAP or RADIUS (see next section), and a login attempt is successful but no user group is returned by the remote authentication server.
UNKNOWN	Permissions defined for this group are employed for a user when your Dominion KX is configured for remote authentication via LDAP or RADIUS (see next section), and a login attempt is successful but the user group returned by the remote authentication server is not found in Dominion KX.

Create or Edit User Groups and Access Permissions

Define User Groups before creating individual Users. When creating a user, you must assign that user to an existing user group. In addition, User Groups are used even if you implement remote authentication (via RADIUS or LDAP).

1. **To create a new User Group**: On the **User** menu, click **Add User Group**. **To edit an existing User Group:** Select the group that you wish to edit in the Navigator, right-click on the icon, and select **Edit User Group**. In both cases, the **Groups** window appears.

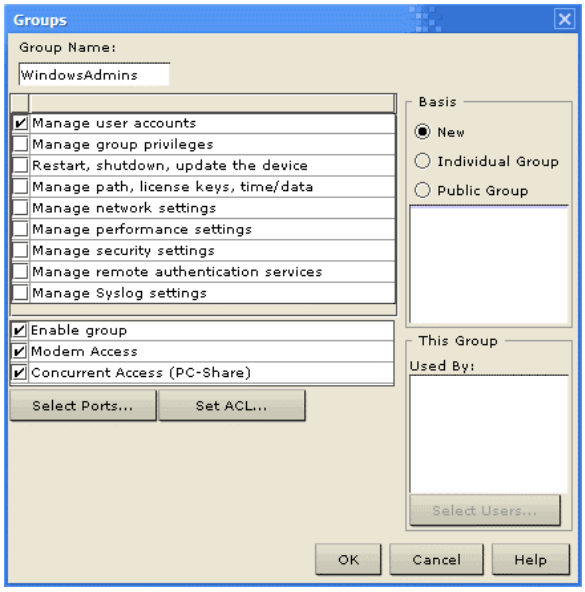

Figure 34 Groups Window

2. Type a name for the new user group, or edit the name for an existing user group in the **Group Name** field.
3. Check the boxes of the permissions you wish to assign to all users who belong to this group.
4. Note these other permission elements:
   - **This Group Used By** field - Displays all users assigned to this group.
   - [**Select Ports**] – Click this button to specify which server ports can be accessed by users who belong to this group. For each server port, users may be allowed to control the connected target server; view the video (but not interact with) the connected target server; or be denied permission altogether.

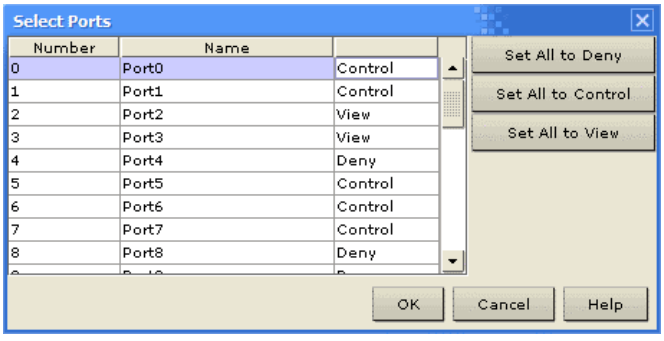

Figure 35 Select Ports Window

– [**Set ACL**] – Click this button to to limit access to Dominion KX by users in this group to specific IP addresses. (This feature applies **only** to users belonging to a specific group, unlike the "Set System ACL" functionality found in the Dominion KX Network Configuration (see previous section **Network Configuration**), which applies to **all** access attempts to Dominion KX.)

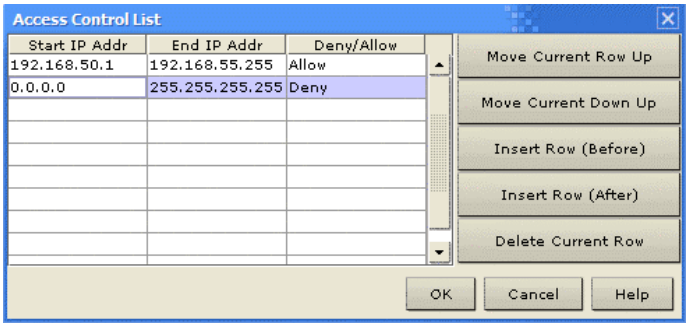

Figure 36 Access Control List Window

Important: Please note that ACL rules are evaluated in the order that they are listed

5. Click [**OK**] to save Group properties or [**Cancel**] to close the window without saving.

Delete User Groups

To delete an existing user group, select the group that you wish to delete, right-click on the group icon, and select **Delete User Group**. Before deleting a group, ensure that there are no users assigned to it, or those users will also be deleted.

Create or Edit Users

1. **To create a new User**: On the **User** menu, click **Add User. To edit an existing User:** Select the user that you wish to edit in the Navigator , right-click on the icon, and select **User Properties**. In both cases, the **Create/Edit User** window appears:

Figure 37 Create/Edit User Window

2. Type a unique user name or edit the existing user name in the **User Name** field.
3. Click on the **Group Name** drop-down arrow and select a User Group to which you want to assign this user. If you do not want to associate this user with an existing User Group, select **Individual Group** from the drop-down list, and then click [**Individual Settings**] to assign access permissions and privileges for this user.
4. Type a new password or edit an existing password in the **Password** field. Retype the password in the **Confirm Password** field.

5. Click [**OK**] to save User properties or [**Cancel**] to close the window without saving.

Delete Users

To delete an existing user, select the user that you wish to delete, right-click on the user icon, and select **Delete User.**

Remote Authentication

Introduction

Note to CommandCenter Users

If you plan to configure Dominion KX to be integrated with and controlled by Raritan's CommandCenter management appliance, this section of the User Manual does not apply to you. When a Dominion KX unit is controlled by CommandCenter, CommandCenter determines the allowed users and groups. Please refer to your CommandCenter User Guide.

Note to Raritan Customers Upgrading from Previous Firmware Versions

If you have previously implemented RADIUS authentication on Raritan products such as Dominion KSX and IP-Reach running legacy firmware versions earlier than v3.2, read this entire section carefully. Beginning with firmware version v3.2 and above, the implementation of external authentication has changed significantly to provide more flexible and powerful configurations.

Supported Protocols

In order to simplify management of usernames and passwords, Dominion KX provides the capability to forward authentication requests to an external authentication server. Dominion KX supports two external authentication protocols: LDAP and RADIUS.

Note on Microsoft Active Directory

Microsoft Active Directory uses the LDAP protocol natively, and can function as an LDAP server and authentication source for Dominion KX. If it has the IAS (Internet Authorization Server) component, a Microsoft Active Directory server can also serve as a RADIUS authentication source.

Remote Authentication Implementation

Priority

When a user tries to authenticate to a Dominion KX unit that is configured for external authentication, Dominion KX first checks its own internal user database for that username. If the username is not found in the Dominion KX internal database, the request is forwarded to the external authentication server.

- **If Username is not found in Dominion KX internal database:** Request is forwarded to external authentication server to determine whether the login is allowed or denied.
- **If Username is found in Dominion KX internal database and Password is correct:** Login is allowed.
- **If Username is not found in Dominion KX internal database and Password is incorrect:** Login is denied; the request does NOT get forwarded to the external authentication server.

Authentication vs. Authorization

When your Dominion KX unit is configured for remote authentication, the external authentication server is used primarily for the purposes of authentication, not authorization.

Authorization is determined by Dominion KX on the basis of user groups. That is, once a given user is allowed to access the Dominion KX system in general (authenticated), that user's specific permission (authorization) is determined by Dominion KX based upon the user's group.

The external authentication server can assist in authorization by informing Dominion KX about the user group to which a user belongs whenever the authentication server approves a given user's login request. The sections **Implementing LDAP Remote Authentication** and **Implementing RADIUS Remote Authentication** that follow explain this in more detail.

This is most easily described via a simple flow diagram:

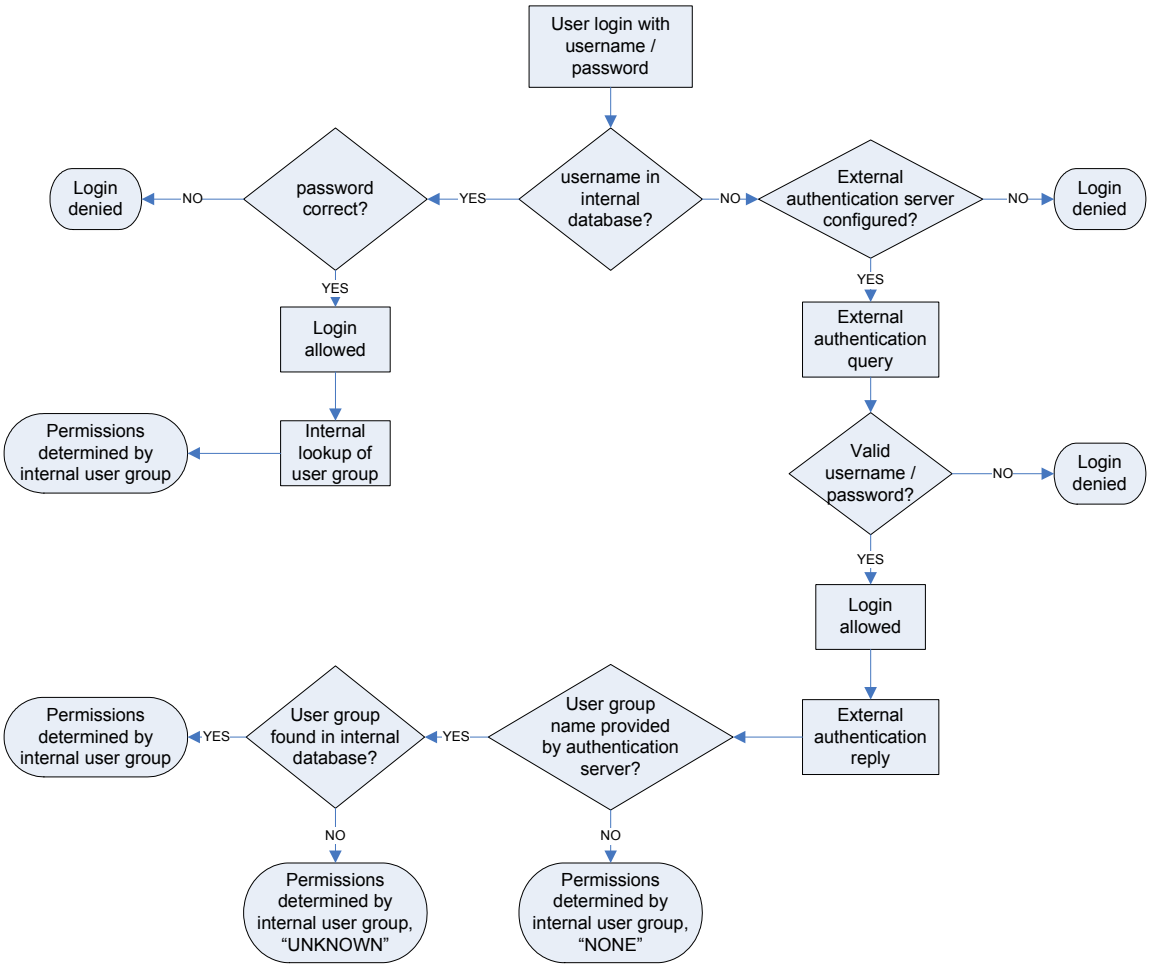

Figure 38 Authorization Flow Diagram

Note the importance of the group to which a given user belongs, as well as the need to configure the groups named, "UNKNOWN" and "NONE." If the external authentication server returns a group name that is not recognized by Dominion KX, that user's permissions are determined by the permanent group named "UNKNOWN." If the external authentication server does not return a group name, that user's permissions are determined by the permanent group named "NONE."

Please see the sections **LDAP** or **RADIUS** in this chapter to determine how to configure your authentication server to return user group information to Dominion KX as part of its reply to an authentication query.

General Settings for Remote Authentication

1. On the **Setup** menu, click **Security**, and then click **Remote Authentication** to configure Dominion KX for remote authentication. The **Remote Authentication** window appears:

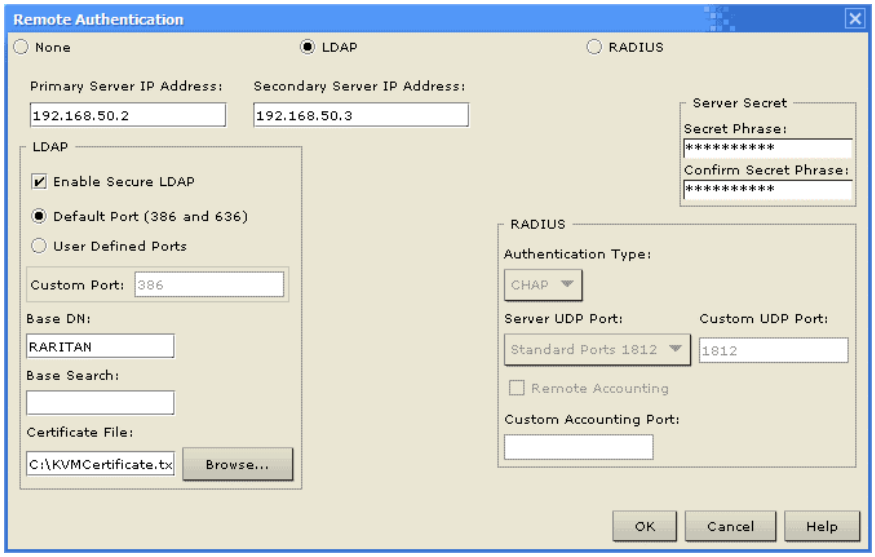

Figure 39 Remote Authentication Window

2. Select the option button of the remote authentication protocol you wish to use (either **LDAP** or **RADIUS**).
3. Enter the IP Address of your primary and secondary remote authentication servers in the **Primary Server IP Address** and **Secondary Server IP Address** fields.
4. Enter the server secret needed to authenticate against your remote authentication servers in the **Secret Phrases** field. Re-type the server secret in the **Confirm Secret Phrase** field.
5. If you selected LDAP as your remote authentication protocol, please read the next section **Implementing LDAP Remote Authentication** to complete the fields in the LDAP panel of the Remote Authentication window. If you selected RADIUS, please skip to **Implementing RADUIS Remote Authentication** to complete the fields in the RADIUS panel of the window.
6. When finished, click [**OK**] to save the Remote Authentication changes, or [**Cancel**] to exit without saving.

Implementing LDAP Remote Authentication

Reminder: Microsoft Active Directory functions natively as an LDAP authentication server.

If you choose LDAP authentication protocol, complete the LDAP fields as follows:

- **Use Secure LDAP:** Apply this rule to enables LDAP-S, which ensures that all authentication requests and replies transmitted over the network are encrypted.
- **Default Port / User Defined Port:** Select an option button to choose whether you would like to use the standard LDAP TCP ports, or specify your own user defined port.
- **Base DN, Base Search,** and **Certificate File:** Consult your authentication server administrator for the appropriate values to type into these fields in order to process LDAP authentication queries from Dominion KX.

Returning User Group Information via LDAP

When an LDAP authentication attempt succeeds, Dominion KX determines the permissions for a given user based on the permissions of the user's group. Your remote LDAP server can provide these user group names by returning an attribute named as follows:

```
rciusergroup        attribute type: string
```

This may require a schema extension on your LDAP server. Please consult your authentication server administrator to enable this attribute.

Implementing RADIUS Remote Authentication

Microsoft Active Directory can be used as source information for RADIUS authentication by installing the Windows server component **Internet Authentication Server**.

If you choose RADIUS authentication protocol, complete the RADUIS fields as follows:

- **Authentication Type:** Click on the drop-down arrow to select either CHAP or PAP protocol.
- **Server UDP Port / Custom UDP Port:** Click on the drop-down arrow to select whether you would prefer using standard RADIUS TCP port 1812, the legacy RADIUS TCP port 1645, or type in your own user defined port in the **Custom UDP Port** field.
- **Remote Accounting / Custom Accounting Port:** Click on the check box to send authentication events to a RADIUS accounting server; if so, type the TCP port should be used for transmitting events in the **Custom Accounting Port**.

Returning User Group Information via RADIUS

When a RADIUS authentication attempt succeeds, Dominion KX determines the permissions for a given user based on the permissions of the user's group.

Your remote RADIUS server can provide these user group names by returning an attribute, implemented as a RADIUS *FILTER-ID*. The *FILTER-ID* should be formatted as follows:

```
Raritan:G{GROUP_NAME}
```

where `GROUP_NAME` is a string, denoting the name of the group to which the user belongs.

RADIUS Communication Exchange Specifications

Dominion KX sends the following information to RADIUS server in an authentication query:

ATTRIBUTE	DATA
USER-NAME	The user name entered at the login screen.
USER-PASSWORD	In PAP mode, the encrypted password entered at the login screen.
CHAP-PASSWORD	In CHAP mode, the CHAP protocol response computed from the password and the CHAP challenge data.
NAS-IP-ADDRESS	Dominion KX's IP Address
NAS-IDENTIFIER	The Dominion KX unit name as configured in "Network Configuration" (see previous section).
NAS-PORT-TYPE	The value ASYNC (0) for modem connections and ETHERNET (15) for network connections.
NAS-PORT	Always 0.
STATE	If this request is in response to an ACCESS-CHALLENGE, the state data from the ACCESS-CHALLENGE packet will be returned.
PROXY-STATE	If this request is in response to an ACCESS-CHALLENGE, the proxy state data from the ACCESS-CHALLENGE packet will be returned.

Dominion KX sends the following RADIUS attributes to the RADIUS server with each accounting request:

ATTRIBUTE	DATA
SESSION-TYPE	Either START (1) for log in or STOP (2) for log out.
SESSION-ID	A string containing a unique session name. The name is in the format of "<NAS-IDENIFIER>:<user IP address>:<unique session number>" Example: "Dominion KX:192.168.1.100:122"
USER-NAME	As above.
NAS-IP-ADDRESS	As above.
NAS-IDENTIFIER	As above.
NAS-PORT-TYPE	As above.
NAS-PORT	As above.
FILTER-ID	Any FILTER-ID attributes returned by the RADIUS server during authentication will be sent in each accounting request.
CLASS	Any CLASS attributes returned by the RADIUS server during authentication will be sent in each accounting request.
ACCT-AUTHENTIC	How the user was authenticated. Either RADIUS (1) if the user was authenticated by the RADIUS server or LOCAL (2) if the user was authenticated by Dominion KX's built-in user name database.
TERMINATE-CAUSE	If this is a STOP request, the reason the user was terminated. Either USER_REQUEST (1), LOST_SERVICE (3), SESSION_TIMEOUT (5), or ADMIN_RESET (6).

View Dominion KX Event Log (Status)

On the **Setup** menu, click **Status** to view the Dominion KX Event Log. The Dominion KX Status window appears, displaying events by date and time. Click [**Export**] and browse for a location to save the displayed log file to a text file. Click [**Copy Log**] to copy the display to your clipboard.

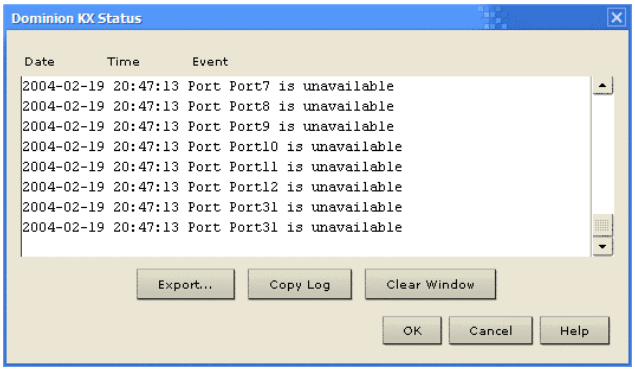

Figure 40 Dominion KX Status Window

Forced User Logoff

To manually log off a user, select that user in the user tree. Right-click on the user icon and select **Logoff User.**

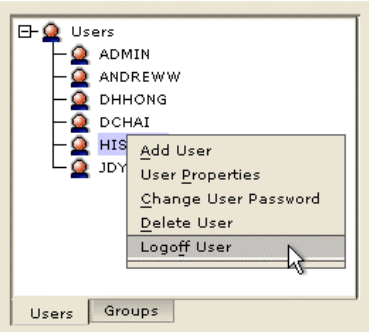

Figure 41 Logoff User Menu, accessed by Right-clicking on User icon

Reboot Dominion KX

On the **Setup** menu, click **Reboot Device** to reboot your Dominion KX unit when in Dominion KX Manager.

Performance Settings

Use this window to set up Dominion KX's video data transfer and bandwidth parameters.

1. On the **Setup** menu, click **Configuration,** and then click **Performance**. The **Performance Setting** window appears.

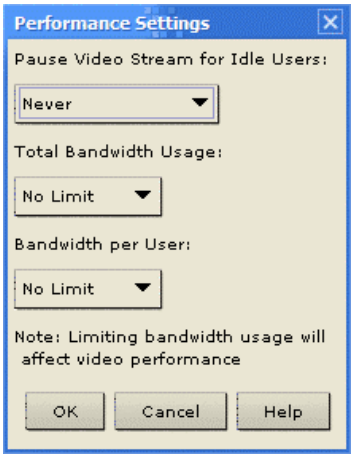

Figure 42 Performance Settings Window

2. **Pause Video Stream for Idle Users**: Click on the drop-down arrow to pause the flow of video data during periods of prolonged inactivity to prevent inactive users from needlessly consuming bandwidth. *Options:* Never / 5 / 15 / 30 / 60 / 120 minutes
3. **Total Bandwidth Usage**: Click on the drop-down arrow to set a maximum amount of bandwidth that can be consumed by this one Dominion KX unit (global). The lower the bandwidth allowed, the slower the performance that may result. *Options:* No Limit / 10Mbps / 5Mbps / 2Mbps / 1Mbps / 512Kbps / 256Kbps / 128Kbps
4. **Bandwidth per User**: Click on the drop-down arrow to set a maximum amount of bandwidth that can be consumed by each user logged onto this one Dominion KX unit. *Options:* No Limit / 10MBits / 5MBits / 2MBits / 1MBits / 512kbit / 256kbit / 128kbit
5. Click [**OK**] to set Performance Settings, or [**Cancel**] to close the window.

Time and Date

Use this window to set Dominion KX's internal clock that timestamps all logged events.

1. On the **Setup** menu, click **Configuration**, and then click **Time/Date**. The **Time and Date** window appears.

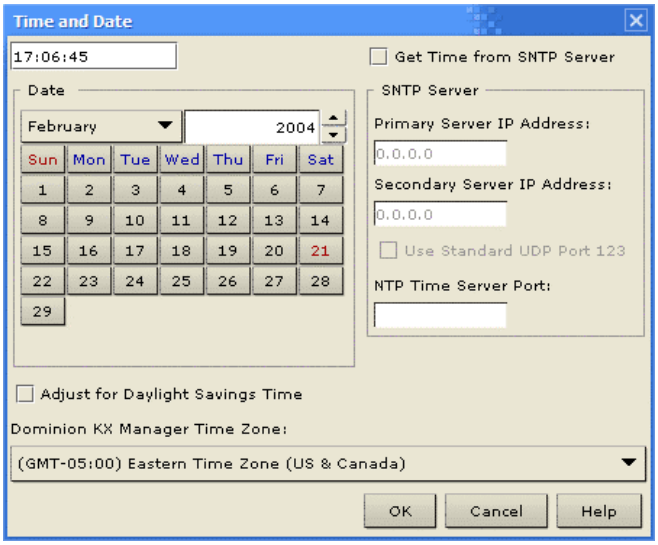

Figure 43 Time and Date Window

On the top-left, you will find the current time and date of your Dominion KX system clock.

2. **Get Time From SNTP Server:** Click on this check box to instructs Dominion KX to synchronize its internal clock with an external time server using SNTP.
   a. Enter the IP address of the primary and secondary SNTP server to which Dominion KX should synchronize in the **Primary Server IP Address** and **Secondary Server IP Address** fields.
   b. If your SNTP server uses a port other than the standard UDP port 123, type the port in the **NTP Time Server Port** field.

If you choose not to use SNTP to synchronize the internal Dominion KX clock, select a month from the drop-down list, a year using the up/down arrow keys, and click on the date in the Date panel.

3. Click [**OK**] to set Time and Date, or [**Cancel**] to close the window.

Chapter 5: Local Console Port Access

Local Port Functionality

When you are located at the server rack, Dominion KX provides standard KVM switch functionality via its Local Console Ports, which features an On-Screen Display (OSD) for quick, convenient switching between servers. The Dominion KX Local Console Port provides a direct analog connection to your connected servers; the performance is exactly as if you were directly connected to the server's keyboard, mouse, and video ports.

Physical Connections

Local Console Ports can be found on the rear panel of the Dominion KX.

Figure 44 Local User Panel on Dominion KX

Monitor: Attach a standard multisync VGA monitor to the HD15 (F) video port.

Keyboard: Attach *either* a standard PS/2 keyboard to the Mini-DIN6 (F) keyboard port *or* a standard USB mouse to one of the USB Type A (F) ports.

Mouse: Attach *either* a standard PS/2 mouse to the Mini-DIN6 (F) mouse port *or* a standard USB mouse to one of the USB Type A (F) ports.

Note: *USB keyboard and mouse ports are to be used only for keyboard and mouse access – other USB devices such as external drives, scanners, etc. should not be connected to these ports.*

Simultaneous Users

The Dominion KX Local Console Port provides an independent access path to your connected servers. Using the Local Console Port does not prevent users from simultaneously connecting over the network, and even when users have connected to Dominion KX over the network, you may still simultaneously access your servers from the rack via the Local Console Port.

Security and Authentication

To use the Dominion KX Local Console Port, first authenticate with a valid username and password. Dominion KX provides a fully-integrated authentication and security scheme, whether you access Dominion KX via the network or via the Local Console Port. In both cases, users use the same username and password, and Dominion KX allows access only to those servers to which a user has access permissions (see **Chapter 4** for more information on creating server access and security settings).

If your Dominion KX has been configured for external authentication services (LDAP, Active Directory, RADIUS, Raritan's CommandCenter management appliance), authentication attempts at the Local Console Port also are authenticated against the external authentication service.

Selecting Servers

Accessing the OSD

To select a server for controlling at the Local Console Port, access the OSD:

- **If you are presently logged out of the Local Console Port:** Type a valid username and password, and the OSD appears.
- **If a server is presently already selected:** Press the OSD "Hot Key" <**Scroll Lock**> twice rapidly to access the OSD.

Important: The Local Console Port OSD Hotkey is <Scroll Lock> <Scroll Lock>.

Server Display Options

While you operate the Local Console Port, Dominion KX will display a list of those servers to which you have permission to access.

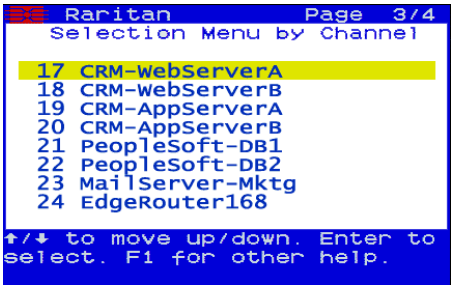

Figure 45 Local Server Display

Your servers can be sorted and displayed by two different parameters:

- **Select by Channel:** Press <**F2**> while in the OSD to display your servers listed in numerical order, as determined by the physical Dominion KX server port to which they are connected.
- **Select by Name:** Press <**F12**> while in the OSD to display your servers listed in alphabetical order by name.

Access a Server

While viewing the Server Display in the OSD, press the <↑> and <↓> arrow keys to scroll through the list of servers. Eight servers are listed per page, and if your list spans multiple pages, press the <**PgUp**> and <**PgDown**> keys to scroll between screens.

Select a server (when the server is highlighted with the yellow bar) you want to access and press <**ENTER**>. The OSD disappears and you are connected directly to the server you have selected.

To return to the OSD, press the "hotkey" (<**Scroll Lock**>) twice rapidly.

Local Port Administration

Dominion KX should ideally be managed via Dominion KX Manager (see **Chapter 4: Administrative Functions**, ***Launching Dominion KX Manager***). However, the Dominion KX Local Console Port provides access to select administrative functions. Only users with administrative privileges can access these functions, via the Administrative Functions menu.

Rename Servers

Assign names to the servers connected to Dominion KX from the Local Console Port, while you are physically located next to the servers themselves.

1. Log on to Dominion KX as a user with administrative privileges, and press <**F5**> to activate the **Administrative Menu**.

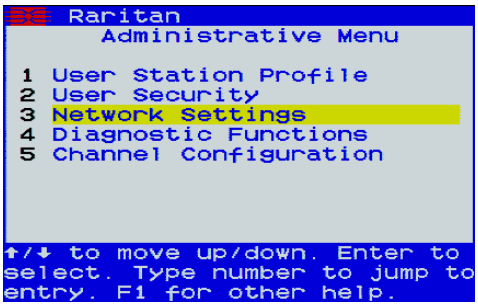
Raritan
Administrative Menu
1 User Station Profile
2 User Security
3 Network Settings
4 Diagnostic Functions
5 Channel Configuration
↑/↓ to move up/down. Enter to select. Type number to jump to entry. F1 for other help.

Figure 47 Administrative Menu

2. Select Option 5, **Channel Configuration**. The **Channel Configuration** menu appears.

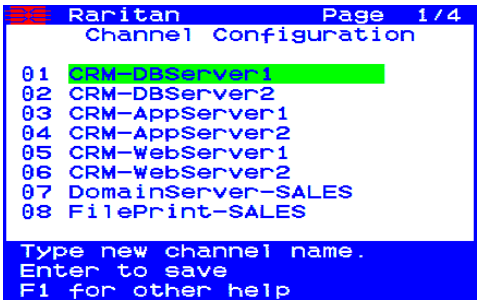

Figure 48 Channel Configuration Menu

3. Use the <↑> and <↓> keys to select a server port to rename, and press <**ENTER**>.
4. When the highlight turns green, type a name (up to 20 characters) to identify the server connected to that port.
5. Press <**ENTER**> to complete.
6. Press <**S**> to save the change, and then press <**ESC**> to exit the menu.

Change Network Settings

1. Log on to Dominion KX as a user with administrative privileges, and press <**F5**> to activate the **Administrative Menu**.
2. Select Option 3, **Network Settings**. The **Network Settings** menu appears.

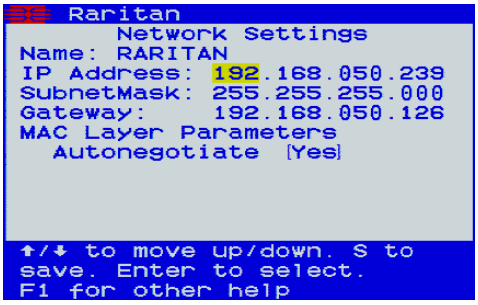

Figure 49 Network Settings Menu

3. Use the <↑> and <↓> keys to navigate through the menu. To edit a setting, press <**ENTER**>. When the highlight turns green, that setting can be edited; use numerical keys as well as the <↑> and <↓> arrow keys to change values.
4. Press <**S**> to save changes, and then press <**ESC**> to exit the menu.

Important: Dominion KX must be rebooted for new network settings to take effect.

Help Menu

To get information or help about the OSD of the Dominion KX Local Console Port, press <**F1**>. The Help Menu appears.

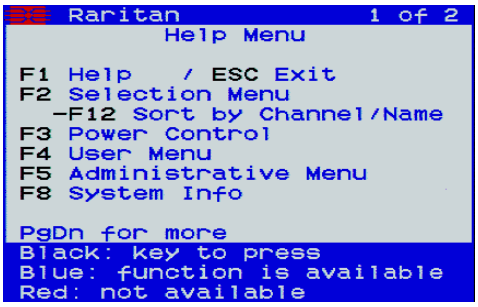

Figure 50 Help Menu

Hardware / Firmware Information

If you need hardware and firmware information specific to your Dominion KX unit, log into the Local Console Port of your Dominion KX unit, and press <**F8**>. The **System Information** screen appears.

Figure 51 System Information Window

Appendix A: Specifications

Digital KVM Switches

PART NUMBER	PRODUCT WEIGHT	PRODUCT DIMENSIONS (WXDXH)	SHIPPING WEIGHT	SHIPPING DIMENSIONS (WXDXH)
DKX116	8.65lb 3.92kg	17.3” x 11.4” x 1.75” 439.41mm x 289.56mm x 44.44mm	14.55 lbs 6.59kg	22” x 16.6” x 6.5” 558.8mm x 421.64mm x 165.1mm
DKX216	8.65lb 3.92kg	17.3” x 11.4” x 1.75” 439.41mm x 289.56mm x 44.44mm	14.55 lbs 6.59kg	22” x 16.6” x 6.5” 558.8mm x 421.64mm x 165.1mm
DKX232	9.0lb 4.08kg	17.3” x 11.4” x 1.75 439.41mm x 289.56mm x 44.44mm	14.9 lbs 6.75kg	22” x 16.6” x 6.5” 558.8mm x 421.64mm x 165.1mm

Computer Interface Modules (CIMs)

PART NUMBER	PRODUCT WEIGHT	PRODUCT DIMENSIONS (WXDXH)	SHIPPING WEIGHT	SHIPPING DIMENSIONS (WXDXH)
DCIM-PS2	0.2 lbs .09kg	1.3” x 3.0” x 0.6” 33.02mm x 76.19mm x 15.23mm	0.2 lbs .09kg	7.2” x 9” x 0.6” 182.88mm x 228.6mm x 15.23mm
DCIM-USB	0.2 lbs .09kg	1.3” x 3.0” x 0.6” 33.02mm x 76.19mm x 15.23mm	0.2 lbs .09kg	7.2” x 9” x 0.6” 182.88mm x 228.6mm x 15.23mm
DCIM-SUSB	0.2 lbs .09kg	1.3” x 3.0” x 0.6” 33.02mm x 76.19mm x 15.23mm	0.2 lbs .09kg	7.2” x 9” x 0.6” 182.88mm x 228.6mm x 15.23mm
DCIM-SUN	0.2 lbs .09kg	1.3” x 3.0” x 0.6” 33.02mm x 76.19mm x 15.23mm	0.2 lbs .09kg	7.2” x 9” x 0.6” 182.88mm x 228.6mm x 15.23mm

Remote Connection

Network: 10BASE-T, 100BASE-TX Ethernet
Modem: Dedicated Modem Port (DB9M) for External Serial Modem
Qualified for use with US Robotics external serial modems
(as of press date – check Raritan website for latest manual with updated modem certifications).
Protocols: TCP/IP, UDP, SNTP, HTTP, HTTPS, RADIUS, LDAP, LDAPS

Raritan Remote Client (RRC) Applet

Operating System Requirements: Windows XP / NT* / ME / 2000 / 2003 with DirectX.

* Windows NT support for some international keys are limited due to limited Microsoft support for DirectX on the Windows NT platform

Dominion KX Manager (Remote Administration Applet)

Sun Java Runtime Environment (JRE) 1.4.x or later.

TCP Ports Used

- **HTTP, Port 80 (optional)** – All requests received by Dominion KX via HTTP (port 80) are automatically forwarded to HTTPS for complete security. Dominion KX responds to Port 80 for user convenience, relieving users from having to explicitly type "Https://" in the URL field to access Dominion KX, but while still preserving complete security.
- **HTTPS, Port 443 (optional)** – This port is used for a single purpose only: to send the Dominion KX web-accessible clients (Raritan Remote Client and Dominion KX Manager) to the user. No other communication occurs on this port. If you do not wish to use Dominion KX's web-access capabilities and instead prefer to use the installed client software provided on CD-ROM, you can prevent access to Port 443 via your firewall and Dominion KX can still function.
- **Dominion KX (Raritan KVM Over IP) Protocol, Configurable Port 5000 –** With the exception of the above, all communication to Dominion KX occurs over a single, configurable TCP Port. By default, this is set to Port 5000, but you may configure it to use any TCP port of your choice (except 80 and 443). For details on how to configure this setting, please see **Chapter 4: Administrative Functions, *Network Configuration***.
- **SNTP (Time Server) on Configurable UDP Port 123 (optional)** – Dominion KX offers the optional capability to synchronize its internal clock to a central time server. This function requires the use of UDP Port 123 (the standard for SNTP), but can also be configured to use any port of your designation.
- **LDAP on Configurable Ports 386 and 636 (optional)** – If Dominion KX is configured to remotely authenticate user logins via the LDAP protocol, ports 386 and 636 will be used, but the system can also be configured to use any port of your designation.
- **RADIUS on Configurable Port 1812, 1645, or custom port (optional)** – If Dominion KX is configured to remotely authenticate user logins via the RADIUS protocol, either port 1812 or 1645 will be used, but the system can also be configured to use any port of your designation.
- **RADIUS Accounting on Configurable Port** – If Dominion KX is configured to remotely authenticate user logins via the RADIUS protocol, and also employs RADIUS accounting for event logging, an additional port of your designation will be used to transfer log notifications.

KVM Input

Keyboard: PS/2
Mouse: PS/2
Video: VGA

Maximum Cabling Distance: 50 feet (15m) from Computer Interface Module to Dominion KX unit.

Supported Resolutions:

640 x 480 @ 60Hz	1024 x 768 @ 60Hz
640 x 480 @ 72Hz	1024 x 768 @ 70Hz
640 x 480 @ 75Hz	1024 x 768 @ 75Hz
640 x 480 @ 85Hz	1024 x 768 @ 77Hz
	1024 x 768 @ 85Hz
720 x 400 @ 70Hz	
720 x 400 @ 85Hz	1152 x 864 @ 60Hz
	1152 x 864 @ 70Hz
800 x 600 @ 56Hz	1152 x 864 @ 75Hz
800 x 600 @ 60Hz	
800 x 600 @ 72Hz	1152 x 900 @ 66Hz
800 x 600 @ 75Hz	
800 x 600 @ 85Hz	1280 x 960 @ 60Hz
	1280 x 1024 @ 60Hz

Appendix B: Frequently Asked Questions

General Questions

QUESTION	ANSWER
What is Dominion KX?	Dominion KX is a digital KVM (keyboard / video / mouse) switch that enables IT administrators to access and control 16 or 32 servers over the network with BIOS-level functionality. Dominion KX is completely hardware and OS-independent; users can troubleshoot and reconfigure servers even when servers are down. At the rack, Dominion KX provides the same functionality, convenience, space savings, and cost savings as do traditional analog KVM switches. However, Dominion KX also integrates the industry's highest-performing KVM Over IP technology, thereby allowing multiple administrators to access server KVM consoles from any networked workstation in the world.
How does Dominion KX differ from remote control software?	When using Dominion KX remotely, the interface, at first glance, may seem similar to remote control software such as PC Anywhere, Windows Terminal Services / Remote Desktop, VNC, etc. However, because Dominion KX is not a software but a hardware solution, it is much more powerful: OS and hardware independent – Dominion KX can be used to manage any type of server running any OS, whether Intel, Sun, PowerPC running Windows, Linux, Solaris, Novell, etc. State-independent / Agent-less – Dominion KX does not require the managed server OS to be up and running, nor does it require any special software to be installed on the managed server. Out-of-Band – Even if the managed server's own network connection is unavailable, it can still be managed through Dominion KX. BIOS-level access – Even if the server is hung at boot up, requires booting to safe mode, or requires system BIOS parameters to be altered, Dominion KX still works flawlessly to enable these configurations to be made.

Remote Access

QUESTION	ANSWER
How many users can remotely access servers on each Dominion KX?	Currently, Dominion KX models offer concurrent transmissions of up to two unique servers at any time. Dominion KX can, thereby, provide any of the following permutations: • 1 User, viewing two unique servers simultaneously • 2 Users, each viewing unique servers simultaneously • 8 Users – four viewing one server; four viewing a different server simultaneously • Any other permutations of up to 8 users, viewing up to 2 unique servers total.
Can two people look at the same server at the same time?	Yes, up to eight people can look at the same server at the same time.

<table>
<tr><th></th><th></th></tr>
<tr><td>In order to access Dominion KX from a client, what hardware, software, or network configuration is required?</td><td>Because Dominion KX is completely Web-accessible; it does not require proprietary software to be installed on clients used for access. (Although an optional installed client is provided in the box for the purposes of accessing Dominion KX via modem).

Dominion KX can be accessed through any major Web browser including: Internet Explorer, Netscape, and Mozilla. Currently, Dominion KX requires that the Web browser run on a Win32 platform with permissions to launch and execute an ActiveX control.

Dominion KX administrators can also perform remote management (set passwords and security, rename servers, change IP address, etc.). To perform remote management from a given workstation, you must also have Java Runtime Environment of v1.4.x or later installed.</td></tr>
<tr><td>What is the file size of the applet used to access Dominion KX? How long does it take to retrieve?</td><td>The applet used to accessed Dominion KX is approximately 1.4MB in size. The following chart describes the time required to retrieve Dominion KX’s applet at different network speeds:
<table>
<tr><td>100Mbit/s</td><td>Theoretical 100Mbit network speed</td><td>0.1 seconds</td></tr>
<tr><td>60Mbit/s</td><td>Likely practical 100Mbit network speed</td><td>0.2 seconds</td></tr>
<tr><td>10Mbit/s</td><td>Theoretical 10Mbit network speed</td><td>1.1 seconds</td></tr>
<tr><td>6Mbit/s</td><td>Likely practical 10Mbit network speed</td><td>2 seconds</td></tr>
<tr><td>512kBit/s</td><td>Cable modem download speed (typical)</td><td>22 seconds</td></tr>
<tr><td>56kBit/s</td><td>Dial-up modem theoretical speed</td><td>3 minutes</td></tr>
<tr><td>38kBit/s</td><td>Likely practical dial-up modem speed</td><td>5 minutes</td></tr>
</table></td></tr>
<tr><td>How do I access servers connected to Dominion KX if the network ever becomes unavailable?</td><td>Dominion KX offers a dedicated modem port for attaching an external modem. With this dedicated modem, your servers can still be remotely accessed in the event of a network emergency. Furthermore, Dominion KX’s local ports always allow access to your servers from the rack, no matter the network condition.</td></tr>
</table>

Ethernet Networking

<table>
<tr><th>QUESTION</th><th>ANSWER</th></tr>
<tr><td>How much bandwidth does Dominion KX require?</td><td>Dominion KX offers integrated IP-Reach™ technology – the very best video compression available. Raritan has received numerous technical awards confirming its high video quality transmissions and the low bandwidth utilization.

Raritan pioneered the KVM Over IP functionality that allows users to tailor their video parameters to conserve network bandwidth. For instance, when connecting to Dominion KX through a dial-up modem connection, video transmissions can be scaled to grayscale – allowing you to be fully productive while ensuring high performance.

With that in mind, the following data refers to Dominion KX at its default video settings – again, these settings can be tailored to your environment. They can be increased to provide even higher quality video (color depth), or decreased to optimize for low-speed connections.

As a general rule, a conservative estimate for bandwidth utilization (at Dominion KX's default settings) is approximately 0.5Mbit/seconds per active KVM user (connected to and using a server), with very occasional spikes up to 2MBit/seconds. This is a very conservative estimate because bandwidth utilization will typically be even lower.

Bandwidth required by each video transmission depends on what task is being performed on the managed server. The more the screen changes, the more bandwidth is utilized. The table below summarizes some use cases and the required bandwidth utilization at Dominion KX's default settings on a 10Mbit/s network:

<table>
<tr><td>Idle Windows Desktop</td><td>0 Mbit/s</td></tr>
<tr><td>Move Cursor Around Desktop</td><td>0.18Mbit/s</td></tr>
<tr><td>Move Static 400x600 Window/Dialog Box</td><td>0.35Mbit/s</td></tr>
<tr><td>Navigate Start Menu</td><td>0.49Mbit/s</td></tr>
<tr><td>Scroll an Entire Page of Text</td><td>1.23Mbit/s</td></tr>
<tr><td>Run 3D Maze Screensaver</td><td>1.55Mbit/s</td></tr>
</table>
</td></tr>
<tr><td>What is the slowest connection (lowest bandwidth) over which Dominion KX can operate?</td><td>The slowest connection is 20kbits per second (a slow dial-up modem).</td></tr>
<tr><td>What is the speed of Dominion KX's Ethernet interfaces?</td><td>Dominion KX offers two 10/100 speed Ethernet interfaces, with configurable speed and duplex settings (either auto-detected or manually set). Dominion KX does not require a gigabit Ethernet interface because its output (see above question) would never even come close to exceeding the 100Mbit/sec limit of 10/100 Ethernet networking.</td></tr>
<tr><td>Can I access Dominion KX over a wireless connection?</td><td>Yes. Dominion KX not only utilizes standard Ethernet, but also uses very conservative bandwidth with very high quality video. Thus, if you have a wireless client with network connectivity to Dominion KX, you can configure and manage your servers at BIOS-level wirelessly.</td></tr>
<tr><td>Can Dominion KX used over the WAN (Internet), or just over the corporate LAN?</td><td>Yes. Whether via a fast corporate LAN, the less predictable WAN (Internet), a cable modem, or dial-up modem, Dominion KX's KVM Over IP technology can accommodate your connection. Raritan's IP-Reach KVM Over IP technology is integrated into every Dominion KX unit. Raritan pioneered configurable video compression technology, leading the industry by years, as evidenced by its awards.</td></tr>
</table>

Can I use Dominion KX with a VPN?	Yes. Dominion KX uses standard Internet technologies from Layer 1 through Layer 4. Traffic can be easily tunneled through any standard VPN.
How many TCP ports must be open on my firewall in order to enable network access to Dominion KX? Are these ports configurable?	Only one. Dominion KX protects your network security by only requiring access to a single TCP port to operate. This port is completely configurable for additional security. Note that, of course, to utilize Dominion KX's optional Web browser capability, the standard HTTPS port 443 must also be open.
Does the secondary network port provide redundant fail-over, or load balancing?	Currently the secondary network port provides redundant fail-over capabilities: should the primary Ethernet port (or the switch/router to which it is connected) fail, Dominion KX will fail-over to the secondary network port with the same IP address – ensuring that your server operations are not disrupted.
Can Dominion KX be rack mounted?	Yes, Dominion KX ships standard with 19" rack mount brackets. It can also be reverse rack mounted such that the server ports face forward.
How large is Dominion KX?	Dominion KX is only 1U in height, fits in a standard 19" rack mount, and occupies only 11.4" (29 cm) in depth
Does Dominion KX require an external authentication server to operate?	No. Dominion KX is a completely self-sufficient appliance. After assigning an IP address to Dominion KX, it is ready to use – with web browser and authentication capabilities completely built-in. Of course, should you desire to use an external authentication server (such as LDAP, Active Directory, RADIUS, etc.), Dominion KX allows you to, and will even fail-over to its own internal authentication should your external authentication server become unavailable. In this way, Dominion KX's design philosophy is optimized to provide ease of installation, complete independence from any external server, and maximum flexibility.

Servers

QUESTION	ANSWER
Does Dominion KX depend on a Windows server to operate?	Absolutely not. Because you depend on your KVM infrastructure to always be available in any scenario whatsoever (as you will likely need to use your KVM infrastructure to fix problems), Dominion KX is designed to be completely independent from any external server. For example, should your data center come under attack from a malicious Windows worm or virus, you will need to use your KVM solution to resolve the situation. Therefore, it is imperative that your KVM solution, in turn, must not rely on these same Windows servers (or any server, for that matter) to be operational in order for the KVM solution to function. To this end, Dominion KX is completely independent. Even if you choose to configure your Dominion KX to authenticate against an Active Directory server – if that Active Directory server becomes unavailable, Dominion KX's own authentication will be activated and fully functional.
Do I need to install a Web server such as Microsoft Internet Information Services (IIS) in order to utilize Dominion KX's Web browser capability?	No. Dominion KX is a completely self-sufficient appliance. After assigning an IP address to Dominion KX, it is ready to use – with Web browser and authentication capabilities completely built-in.
What software do I have to install in order to access Dominion KX from a particular workstation?	None. Dominion KX can be accessed completely via a Web browser. (Although an optional installed client is provided in the box for the purpose of accessing Dominion KX via modem.)
What should I do to prepare a server for connection to Dominion KX?	Servers connected to Dominion KX do not require any software agents to be installed, because Dominion KX connects directly via hardware to servers' keyboard, video, and mouse ports. In order to provide users with the best mouse synchronization during remote connections, however, you must configure your managed servers' mouse settings (principally, the "acceleration" setting) as instructed in the Dominion KX Quick Setup Guide and Manual.
What comes in the Dominion KX box?	(a) Dominion KX unit; (b) Quick Setup Guide; (c) standard 19" rack mount brackets; (d) User manual CD-ROM; (e) Network cable; (f) Crossover cable; (g) Localized AC Line Cord; (h) Warrantee certificate and other documentation.

Installation

QUESTION	ANSWER
Besides the unit itself, what do I need to order from Raritan to install Dominion KX?	For each server that you wish to connect to Dominion KX, you will require a computer interface module (CIM), a very small dongle that connects directly to the keyboard, video, and mouse ports of your server
What kind of Cat5 cabling should be used in my installation?	Dominion KX can use any standard UTP (twisted pair) cabling, whether Cat5, Cat5e, or Cat6. Often in our manuals and marketing literature, Raritan will simply say "Cat5" cabling for short. In actuality, any brand UTP cable will suffice for Dominion KX.
What types of servers can be connected to Dominion KX?	Dominion KX is completely vendor independent. Any server with keyboard, video, and mouse ports can be connected.
How do I connect servers to Dominion KX?	For each server that you wish to connect to Dominion KX, you will require a computer interface module (CIM), a very small dongle that connects directly to the keyboard, video, and mouse ports of your server. Then, connect each dongle to Dominion KX using standard UTP (twisted pair) cable such as Cat5, Cat5e, or Cat6.
How far can my servers be from Dominion KX?	Servers can be up to 50 feet (15 meters) away from Dominion KX.
Some operating systems "lock up" if you disconnect a keyboard or mouse during operation. What prevents servers connected to Dominion KX from "locking up" when users switch away from them?	Each computer interface module (CIM) dongle acts as a virtual keyboard and mouse to the server to which it is connected. This technology is called KME (keyboard/mouse emulation). Raritan's KME technology is data center grade, battle-tested, and far more reliable than that found in lower end KVM switches: it incorporates more than 15-years of experience, has been deployed to millions of servers worldwide.
Are there any agents that must be installed on servers connected to Dominion KX?	Servers connected to Dominion KX do not require any software agents to be installed, because Dominion KX connects directly via hardware to servers' keyboard, video, and mouse ports.
How many servers can be connected to each Dominion KX unit?	Dominion KX models range, offering up to 32 server ports per unit – in a 1U chassis, this is the industry's highest digital KVM switch port density.
What happens if I disconnect a server from Dominion KX and reconnect it to another Dominion KX unit, or connect it to a different port on the same Dominion KX unit?	Dominion KX will automatically update the server port names when servers are moved from port to port. Furthermore, this automatic update does not just affect the local access port, but it propagates to all remote clients and the optional CommandCenter management appliance.
How do I connect a serially controlled (RS-232) device to Dominion KX, such as a Cisco router/switch or a headless Sun server?	If you only have a few serially-controlled devices, you may connect them to Dominion KX using Raritan's serial computer interface module (CIM), Raritan P/N# AUATC. However, if you have four or more serially controlled devices, we recommend the use of Raritan's Dominion SX model line of secure console servers. For multiple serial devices, Dominion SX offers more functionality at a better price point than Dominion KX, while being just as easy to use, configure and manage, and can be completely integrated with your Dominion Series deployment. In particular, many UNIX and networking administrators appreciate the ability to directly SSH to a Dominion SX unit (which Dominion KX, a digital KVM switch, does not offer).

Local Port

QUESTION	ANSWER
Can I access my servers directly from the rack?	Yes, at the rack Dominion KX functions just like a traditional KVM switch – allowing you to control up to 32 servers using a single keyboard, mouse, and monitor.
When I am using the local port, do I prevent other users from accessing servers remotely?	No. The Dominion KX local port has a completely independent access path to the servers. This means a user can access servers locally at the rack – without compromising the number of users that access the rack remotely at the same time.
Can I use a USB keyboard or mouse at the local port?	Yes. Dominion KX offers both PS/2 and USB keyboard and mouse ports on the local rack. Note that the USB ports are USB v1.1, and support keyboards and mice only – not USB devices such as scanners or printers.
How do I select between servers while using the local port? Is there an On-Screen Display (OSD)?	Yes. Dominion KX's local access port displays an on-screen display interface that presents a list of all servers connected to the Dominion KX unit. Users interact with this convenient on-screen display interface to select a connected server.
How do I ensure that only authorized users can access servers from the local port?	Dominion KX offers the very best local port authentication scheme available on the market: users attempting to use the local port must pass the same level of authentication as those accessing remotely. This means that: If you have configured Dominion KX to interact with an external RADIUS, LDAP, or Active Directory server, users attempting to access the local port will authenticate against the same server. If you have configured Dominion KX to be managed by Raritan's CommandCenter management appliance, users attempting to access the local port will authenticate against CommandCenter (which in turn can also integrate with RADIUS, LDAP, Active Directory, or TACACS [see CommandCenter data sheet and FAQ for more details]). In either of the above scenarios, if the external authentication servers are unavailable, Dominion KX fails-over to its own internal authentication database. Dominion KX has its own standalone authentication, enabling instant on, out-of-the-box installation.
If I use the local port to change the name of a connect server, does this change propagate to remote access clients as well? Does it propagate to the optional CommandCenter appliance?	Yes. The local port presentation is identical and completely in sync with remote access clients, as well as Raritan's optional CommandCenter management appliance. To be clear, if you change the name of a server via the Dominion KX on-screen display, this updates all remote clients and external management servers in real-time.
If I use Dominion KX's remote administration tools to change the name of a connected server, does that change propagate to the local port OSD as well?	Yes, if you change the name of a server remotely, or via Raritan's optional CommandCenter management appliance, this update immediately affects Dominion KX's on-screen display.

Power Control

QUESTION	ANSWER
What type of power control capabilities does Dominion KX offer?	Because Dominion KX enables you to remotely manage servers; it also incorporates the critical functionality of hard power control to servers. Instead of using a third-party tool for power control (likely with lower security and fail-safe capabilities as Dominion KX), you can use Dominion KX's fully integrated remote power control. When remotely connected to an appropriately configured Dominion KX, simply select the power control options to hard reboot a hung server. Note that a hard reboot provides the physical equivalent of unplugging the server from the AC power line, and re-inserting the plug.
Does Dominion KX support servers with multiple power supplies? What if each power supply is connected to a different power strip?	Yes. Dominion KX can be easily configured to support multiple power supplies connected to multiple power strips.
Does remote power control require any special server configuration?	Some servers ship with default BIOS settings such that the server does not restart after losing and regaining power. See your server user manual for more details.
What type of power strips does Dominion KX support?	Dominion KX can support any serially controlled power strips supplied by any vendor, by using our Serial (RS-232) computer interface module. However, to take advantage of Dominion KX's integrated power control user interface, and more importantly, integrated security, you must use Raritan's power strips ("remote power control units"). These power strips come in many outlet, connector, and amp variations – simply order any Raritan power strip whose part number ends in the "-PK" designation. The most popular units are: PCR8-15-PK 8 receptacle, 110V, 15A, NEMA 5-15P, NEMA 5-15R, 1U PCR8A-15-PK 8 receptacle, 220V, 10A, IEC320 C14 P, IEC320 C13 R, 1U PCS12-20L-PK 12 receptacle, 110V, 20A, NEMA L5-20P, NEMA 5-15R, "zero-U" PCS12-20-PK 12 receptacle, 110V, 20A, NEMA 5-20P, NEMA 5-15R, "zero-U" PCS12A-20-PK 12 receptacle, 220V, 10A, IEC320 C14 P, IEC320 C13 R, "zero-U" PCS20-20L-PK 20 receptacle, 110V, 20A, NEMA L5-20P, NEMA 5-15R, "zero-U" PCS20-20-PK 20 receptacle, 110V, 20A, NEMA 5-20P, NEMA 5-15R, "zero-U" PCS20A-20-PK 20 receptacle, 220V, 16A, IEC320 C20 P, IEC320 C13 R, "zero-U" PCS20A-60-PK 20 receptacle, -48VDC, 60A, DC Terminal P, DC Terminal R, "zero-U"

Scalability

QUESTION	ANSWER
How do I connect multiple Dominion KX devices together into one solution?	Multiple Dominion KX units do not need to be physically connected together. Instead, each Dominion KX unit connects to the network, and they automatically work together as a single solution: If you deploy Raritan's optional CommandCenter management appliance, CommandCenter acts as a single access point for remote access and management. CommandCenter offers a significant set of convenient tools, such as consolidated configuration, consolidated firmware update, and a single authentication and authorization database. In addition, CommandCenter enables sophisticated server sorting, permissions, and access functionality – for instance, you can create an attribute called "Operating System", and in one step enable only the Active Directory group "SYSADMINS" to access those servers whose "Operating System" attribute is set to "Windows". See CommandCenter data sheet and FAQ for more details. If you do not take advantage of Raritan's optional CommandCenter management appliance, multiple Dominion KX units still interoperate and scale automatically: Dominion KX's remote access applet automatically discovers all Dominion KX units in your network.
Can I connect an existing analog KVM switch to Dominion KX?	Yes. If you would like to add remote access capabilities to your existing analog KVM switch, you can connect your KVM switch to one of Dominion KX's server ports. Simply use a PS/2 Computer Interface Module (CIM), and attach it to the user ports of your existing analog KVM switch. Please note, however, that KVM switches from most other manufacturers do not have as reliable keyboard and mouse emulation technologies as do Raritan KVM switches. Therefore, if your existing analog KVM switch is not a Raritan brand switch, you may occasionally encounter keyboard or mouse aberrations, and as such Raritan cannot certify the use of any particular third-party analog KVM switch.

Computer Interface Modules (CIMs)

QUESTION	ANSWER
Can I use Computer Interface Modules (CIMs) from Raritan's analog matrix KVM switch, Paragon, with Dominion KX?	Yes. For complete interoperability, certain Paragon computer interface modules (CIMs) do work with Dominion KX (please check the Raritan web site for the latest list of certified CIMs). However, because Paragon CIMs cost more than Dominion KX CIMs (as they incorporate technology for video transmission of up to 1000 feet [300 meters]), it is not generally advisable to purchase Paragon CIMs for use with Dominion KX. Also note that when connected to Dominion KX, Paragon CIMs transmit video at a distance of 50feet [15 meters], the same as Dominion KX CIMs – not at 1000 feet [300 meters], as they do when connected to Paragon.
Can I use Z-Series "daisy-chaining" Computer Interface Modules (CIMs) with Dominion KX?	At the present time, Raritan's Z-Series "daisy-chaining" computer interface modules do not work with Dominion KX. This capability will be incorporated in future releases – requiring only a firmware upgrade.
Can I use Dominion KX Computer Interface Modules (CIMs) with Raritan's analog matrix KVM switch, Paragon?	No. Dominion KX computer interface modules (CIMs) transmit video at a range of 50feet (15 meters) and thus do not work with Paragon, which requires CIMs that transmit video at a range of 1000 feet (300 meters). To ensure that all Raritan's customers experience the very best quality video available in the industry – a consistent Raritan characteristic – Dominion Series CIMs do not interoperate with Paragon.

Security

QUESTION	ANSWER
What kind of encryption does Dominion KX use?	Dominion KX utilizes industry-standard (and extremely secure) 128-bit RC4 encryption, both in its SSL communications as well as its own data stream. Literally no data is transmitted between remote clients and Dominion KX that is not completely secured by encryption.
Does Dominion KX allow encryption of video data? Or does it only encrypt keyboard and mouse data?	Unlike competing solutions, which only encrypt keyboard and mouse data, Dominion KX does not compromise your security - it allows encryption of keyboard, mouse and video data.
How does Dominion KX integrate with external authentication servers such as Active Directory, RADIUS, or LDAP?	Through a very simple configuration, Dominion KX can be set to forward all authentication requests to an external server such as LDAP, Active Directory, or RADIUS. For each authenticated user, Dominion KX receives from the authentication server the user group to which that user belongs. Dominion KX then determines the user's access permissions depending on what user group to which he belongs.
How are usernames and passwords stored?	Should you use Dominion KX's internal authentication capabilities, all sensitive information such as usernames and passwords are stored in a hashed format. Literally no one, including Raritan technical support or Product Engineering departments, can retrieve those usernames and passwords.

Manageability

QUESTION	ANSWER
Can Dominion KX be remotely managed and configured via web browser?	Yes. Dominion KX can be completely configured remotely via Web browser. Note that this does require that your workstation have Java Runtime Environment 1.4.x (or later) installed. Besides the initial setting of Dominion KX's IP address, everything about the solution can be completely set up over the network. (In fact, using a crossover Ethernet cable and Dominion KX's can configure even the initial settings configured via Web browser.)
Can I backup and restore Dominion KX's configuration?	Yes, Dominion KX's configuration can be completely backed up for later restoration in the event of a catastrophe. More commonly, this functionality is also very useful for configuring multiple Dominion KX units if you have not deployed Raritan's CommandCenter centralized management appliance (i.e., configure one unit completely, back up its configuration, and then "restore" it to all remaining units). Dominion KX's backup and restore functionality can be utilized remotely over the network; in fact, via a Web browser.
What auditing or logging does Dominion KX offer?	For complete accountability, Dominion KX logs all major user events with a date and time stamp. For instance, reported events include (but are not limited to): user login, user logout, user access of a particular server, unsuccessful login, configuration changes, etc
Can Dominion KX integrate with syslog?	Yes, for your convenience, in addition to Dominion KX's own internal logging capabilities, Dominion KX can also send all logged events to a centralized syslog server.
Can Dominion KX's internal clock be synchronized with a timeserver?	Yes, Dominion KX supports the industry-standard NTP protocol for synchronization with either your corporate timeserver, or with any public time server [assuming that outbound NTP requests are allowed through your corporate firewall].
Does the power supply used by Dominion KX automatically detect voltage settings?	Yes, Dominion KX's power supply can be used in any AC voltage ranges from 88–264 volts, at 47–63 Hz.

Miscellaneous

QUESTION	ANSWER
What is Dominion KX's default IP address?	192.168.0.192
What is Dominion KX's default username and password?	For the highest level of security, Raritan highly recommends that users reconfigure their Dominion KX default administrative username and password of (**admin**/**raritan** [all lower case]) as soon as the unit is connected to the network.
I changed and subsequently forgot Dominion KX's administrative password; can you retrieve it for me?	For the highest level of security, literally nobody can retrieve lost administrative passwords. Contact your regional Raritan technical support department for instructions on how to completely reset your unit to factory default settings.
Is 24/7 Technical Support available for Dominion KX?	Yes.